CWD-854
Wireless-G USB Dongle

User Manual

Version: 1.0.0

(May 2009)

Table of Contents

Chapter 1: Introduction 3

1.1 About CWD-854 3

1.2 Main Features 3

1.3 System Requirements 4

1.4 Getting to Know CWD-854 4

Chapter 2: Driver Installation and Configuration 5

2.1 USB Adapter Installation 5

2.2 Connect to Wireless Access Point 9

Chapter 3 Configuration Utility 12

3.1 Utility Overview 13

3.2 Available Network 14

3.3 General 15

3.4 Profile 16

3.5 Advanced 21

3.6 Status 23

3.7 Statistics 24

3.8 Wi-Fi Protect Setup 25

3.9 Software AP 31

Chapter 4 Set Wizard 38

Chapter 5 Glossary 42

Chapter 1: Introduction

1.1 About CWD-854

The Wireless-G USB Dongle can be installed in most notebooks and provides true flexibility by allowing the computer to be positioned almost anywhere in the building without the cost and hassle of running network cables. Using the wireless-G USB Dongle, you don't have to worry about drilling holes in your walls and climbing through the attic or cellar to get connected to the network. Once installed and connected, you can keep in touch with friends and work through e-mail, instant messaging and chat rooms as well as sharing files and other network resources such as printers and network storage with other computers.

The Wireless-G USB Dongle connects to 802.11g networks at an incredible speed of 54Mbps and for added versatility; it also interoperates with all Wireless-B (802.11b) products found at homes, businesses, and public wireless hotspots around the country.

1.2 Main Features

The following lists the main features of the Wireless-G USB Dongle.

- Complies with IEEE 802.11b and 802.11g standards
- 5 times faster and seamlessly interoperate with existing Wireless-B Equipment
- Support Soft AP function – allowing users to configure the card as AP
- Support 64/128-bit WEP, WPA, WPA2 and 802.1x security
- Support WPS for easy wireless setup
- Support Windows 98SE/ME/2000/XP/Vista

1.3 System Requirements

- An empty USB 2.0 port (May not work on USB 1.1 port, and performance will be greatly reduced)
- Windows 98SE, ME, 2000, XP, or Vista operating system
- CD-ROM drive
- At least 100MB of available disk space

1.4 Getting to Know CWD-854

This section describes and shows the top panel of Wireless-G USB Dongle. An activity LED will blink when the card is receiving or transmitting data.

LED	COLOR	STATUS	DESCRIPTION
ACT	Green	Blinking	When the Dongle transmits/receives data.
		Off	No data is being transmitted or received

Chapter 2: Driver Installation and Configuration

2.1 USB Adapter Installation

Please follow the instructions below to install the wireless USB adapter on your system. The following steps are for systems running on Windows XP. (Procedures are similar for Windows 2000/XP/Vista)

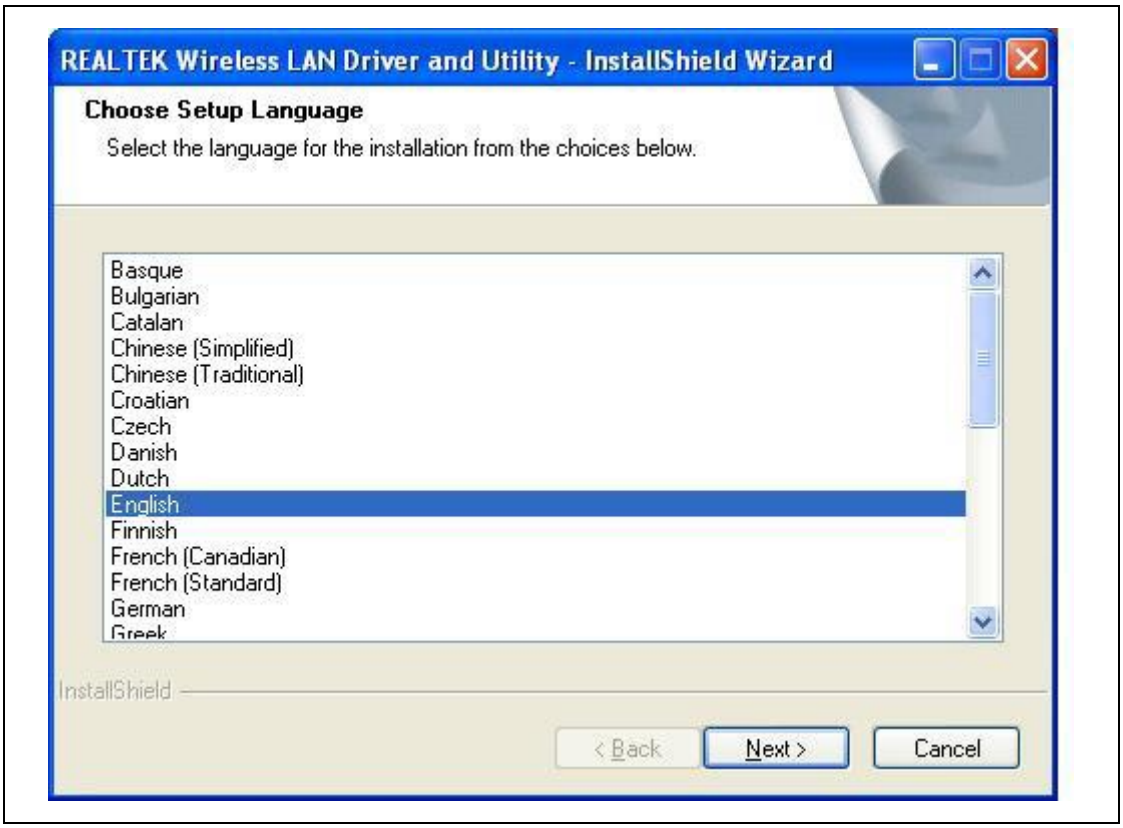
Warning: Do not install the CWD-854 USB Dongle into your computer before installing drivers first.

Insert device driver CD into the CD/DVD ROM drive of your computer.

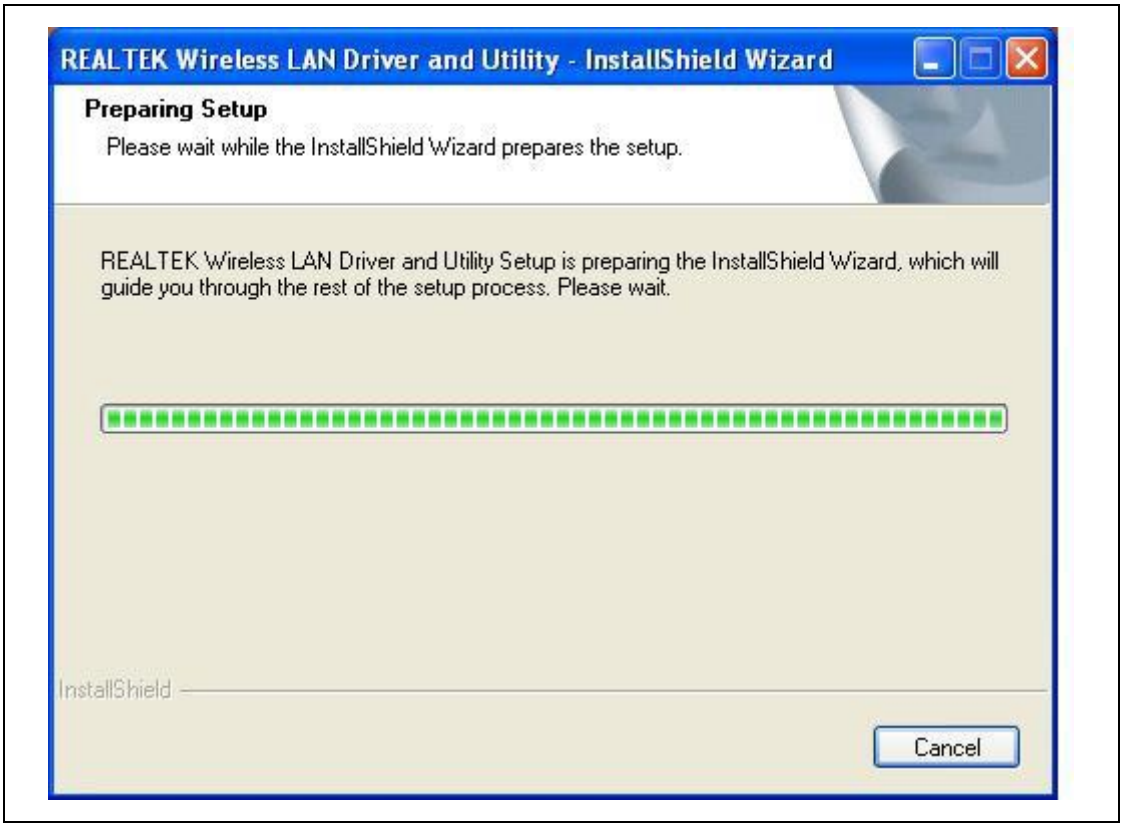
If the CD Auto-Run doesn't automatically start, please go to **Start > Run,** and type "**D:\AUTORUN.exe**" (where D: represents the drive letter of your CD/DVD ROM drive).

1. The main installation screen displays. Click **"DRIVER"** to install CWD-854 Wireless Dongle drivers and utility.

2. Please select the language, which you want to use and click **"Next>"**.



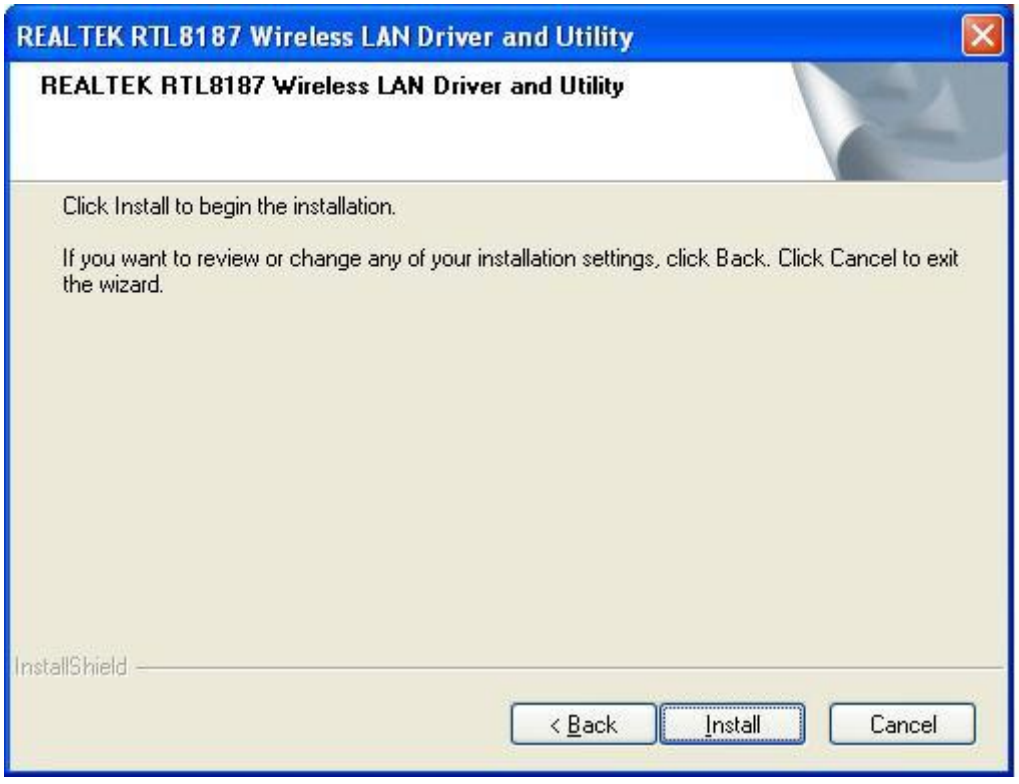
3. The installation process is being prepared.


REALTEK Wireless LAN Driver and Utility - InstallShield Wizard
Preparing Setup
Please wait while the InstallShield Wizard prepares the setup.
REALTEK Wireless LAN Driver and Utility Setup is preparing the InstallShield Wizard, which will guide you through the rest of the setup process. Please wait.
InstallShield
Cancel

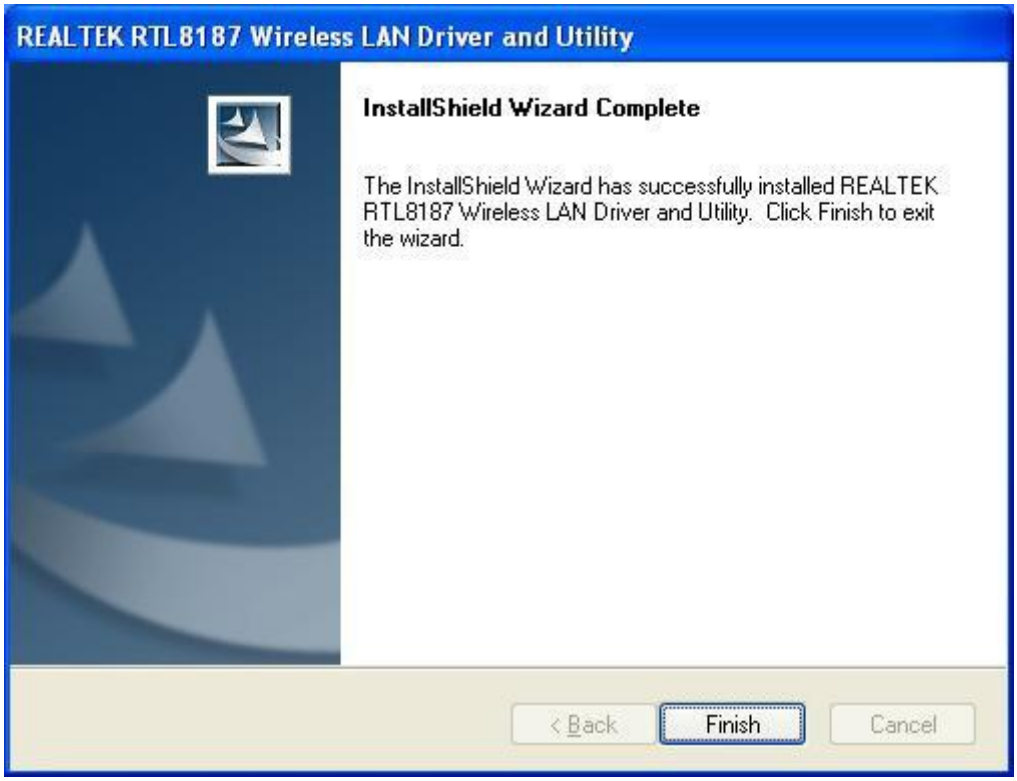
4. Click **"Next>"** to continue or click **"Cancel"** to abort installation.

REALTEK RTL8187 Wireless LAN Driver and Utility
REALTEK RTL8187 Wireless LAN Driver and Utility
The InstallShield Wizard will install REALTEK RTL8187 Wireless LAN Driver and Utility on your computer. To continue, click Next.
< Back
Next >
Cancel

5. Click **"Install"** to begin the installation or click **"Cancel"** to stop process.


REALTEK RTL8187 Wireless LAN Driver and Utility
REALTEK RTL8187 Wireless LAN Driver and Utility
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel

6. Please wait while the install procedure is running. When you see this message, please click **"Finish"** to complete the installation process.

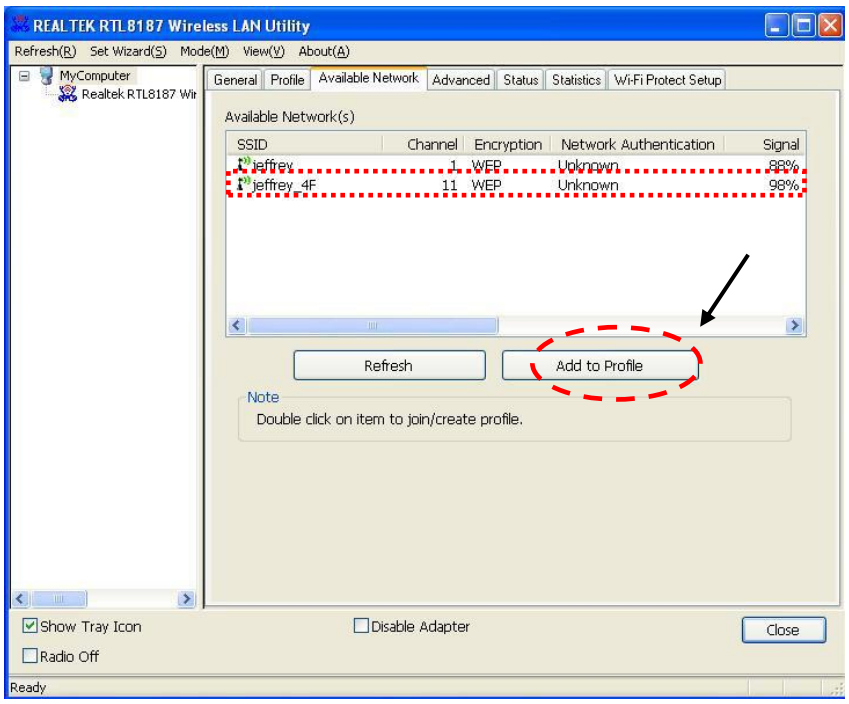

REALTEK RTL8187 Wireless LAN Driver and Utility
InstallShield Wizard Complete
The InstallShield Wizard has successfully installed REALTEK RTL8187 Wireless LAN Driver and Utility. Click Finish to exit the wizard.
< Back
Finish
Cancel

7. Insert the CWD-854 USB Dongle into an empty USB 2.0 port of your computer.

2.2 Connect to Wireless Access Point

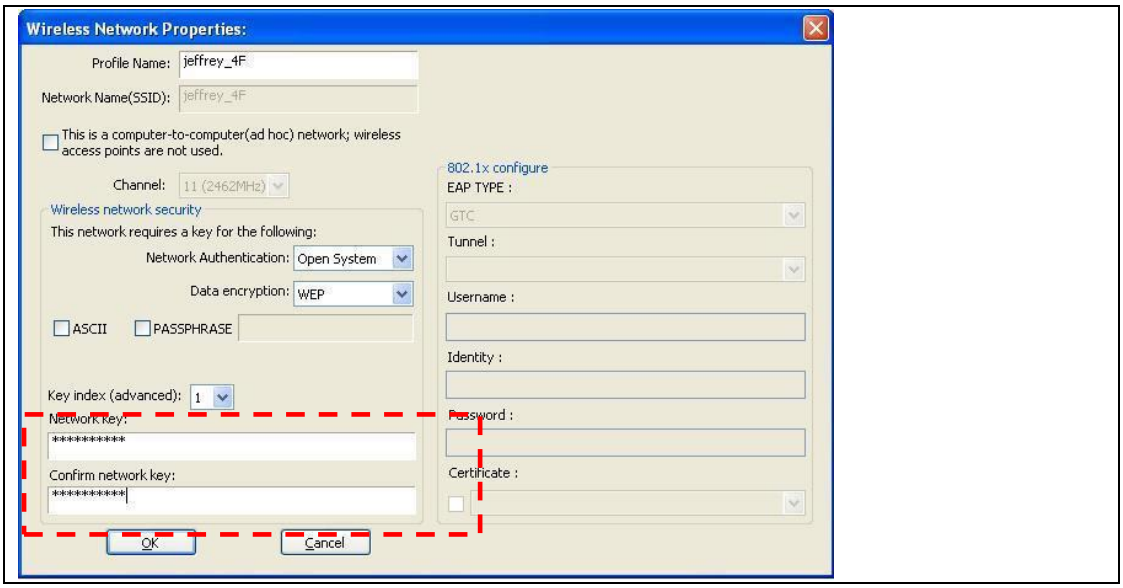
1. After installation is complete, an icon for the wireless configuration utility will be shown on your desktop. Click the icon to bring up the utility.

2. Configuration utility will automatically scan for wireless access points, and display a list of **"Available Networks"**. Please select an access point you wish to connect to, and click **"Add to Profile"**. Click **"Refresh",** if your wireless access point is not shown in the list.

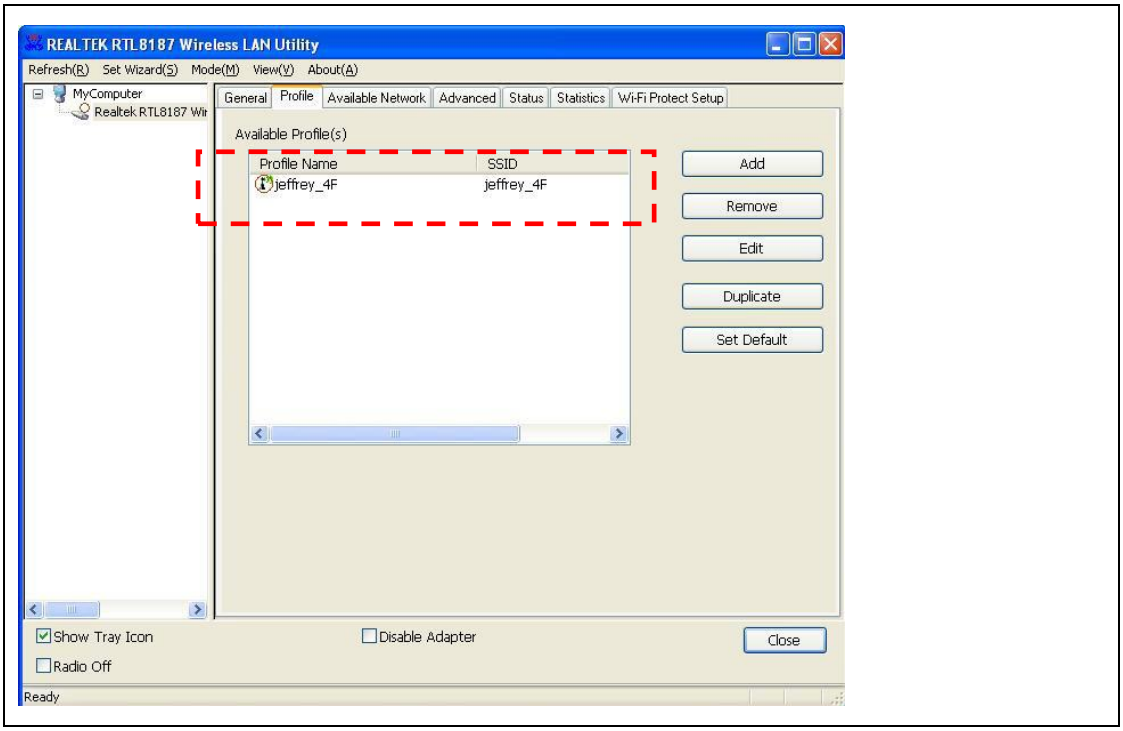


3. If the wireless router/access point you're connecting to is secured through encryption, the security information used on the router must also be entered into this utility. Please contact the network administrator if you don't have the security keys and enter them into this utility. If the security keys don't match, you will not be able access the wireless network.

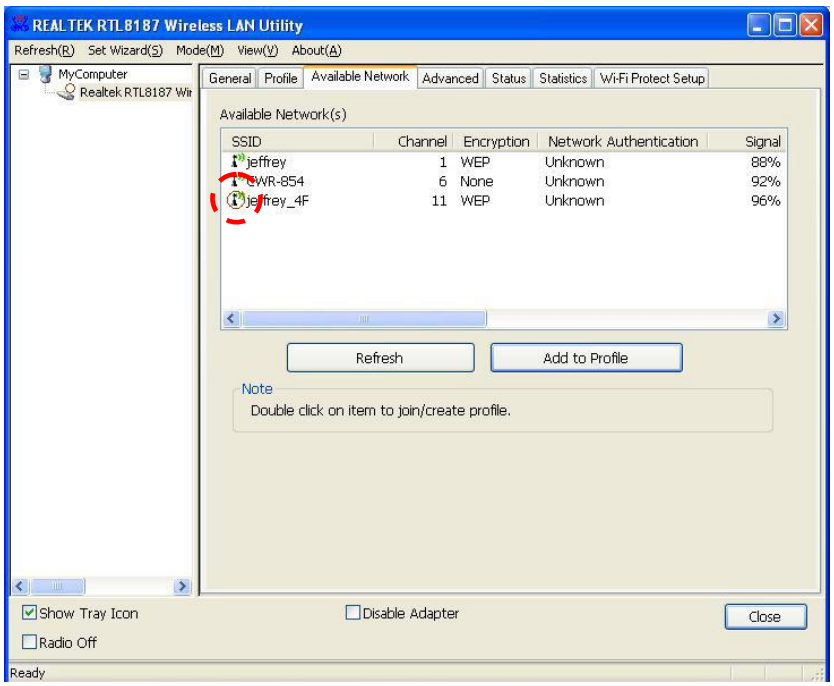
Authentication type is automatically selected, please don't change it.



4. The utility will automatically add the router/access point to a profile list



5. If the wireless connection is successful, a connected icon will display at the lower-left corner of wireless configuration utility. When done, click **"Close"** to exit.



Chapter 3 Configuration Utility

The Configuration Utility is a powerful application that helps configuring the Wireless Dongle as well as monitoring the link status and statistics during the communication process.

The Configuration Utility appears as an icon on the system tray and windows desktop. You can open it by double clicking on the icon.

In the Desktop

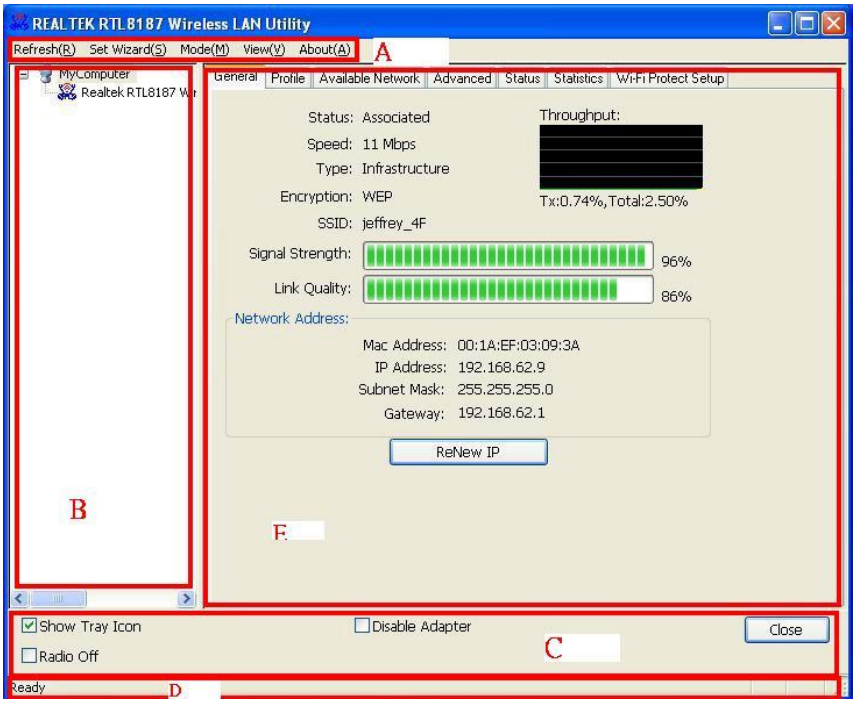
In the System Tray

You could also right click on the icon in the system try to access the configuration utility.

- Open Config Utility: Select **"Open Config Utility"** to open the configuration utility
- Set Wizard: Select **"Set Wizard"** to open RT-Set Wizard
- About: Select **"About"** to show the utility information
- Hide: Select **"Hide"** to hide the utility in the system tray
- QUIT: Select **"QUIT"** to close utility

3.1 Utility Overview

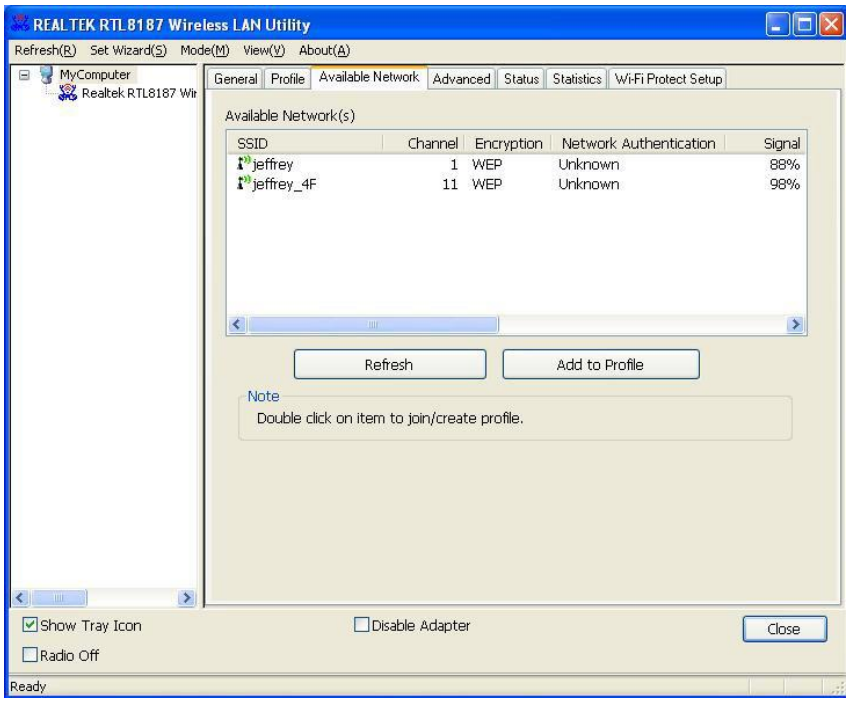
There are several sections in the utility screen. Please use the following table for the description of each section.



Parameter	Description
A	• **Refresh** – Refresh adapter list in the “B” bloc • **Set Wizard** – Open the Setup Wizard • **Mode** – There are two modes: Station and Access Point. If **“Station”** is selected, the adapter works as a wireless adapter. If **“Access Point”** is selected, the adapter works as a wireless AP • **View –** Enable **“Status Bar“** and the “D“ block in the utility will display the current status of the utility • **About --** To check the version of the utility, select this item
B	This is a list of detected wireless adapters on your PC
C	• **Show Tray Icon** -- To show the icon in the system tray. • **Radio Off** -- This function is to turn the radio signal off. If the radio is turned off, the adapter will not work. • **Disable Adapter** – If checked, the adapter is disabled.
D	This is where the status of the card is displayed. To close it, please disable the “Status Bar“ in the “View“ item.
E	This field contains many tabs containing different functions of the adapter. Next Below is a detailed explanation of each tab.

3.2 Available Network

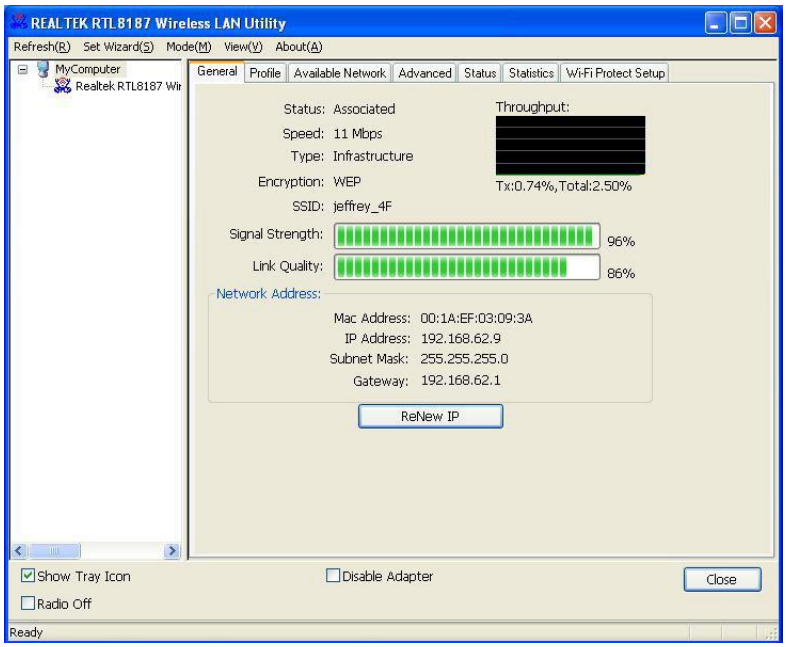
When you open the Configuration Utility, the system will scan all channels to find the available access points/stations within its range and automatically connects to the wireless network with the highest signal strength. In the “Available Network” tab, one can see a list of all nearby networks. You can choose which network to connect to.



Parameter	Description
Available Network(s)	This is a list of all available wireless networks within the range of your adapter. The information for each network includes SSID, Channel, Encryption, Network Authentication, Signal and etc. To connect to any network on the list, just double-click the network.
Refresh	Click **“Refresh“** to update the networks list. It is recommended to refresh the list when network connections are changed.
Add to Profile	A profile stores the setting of a network for faster network connection. Click this button to add a selected network.

3.3 General

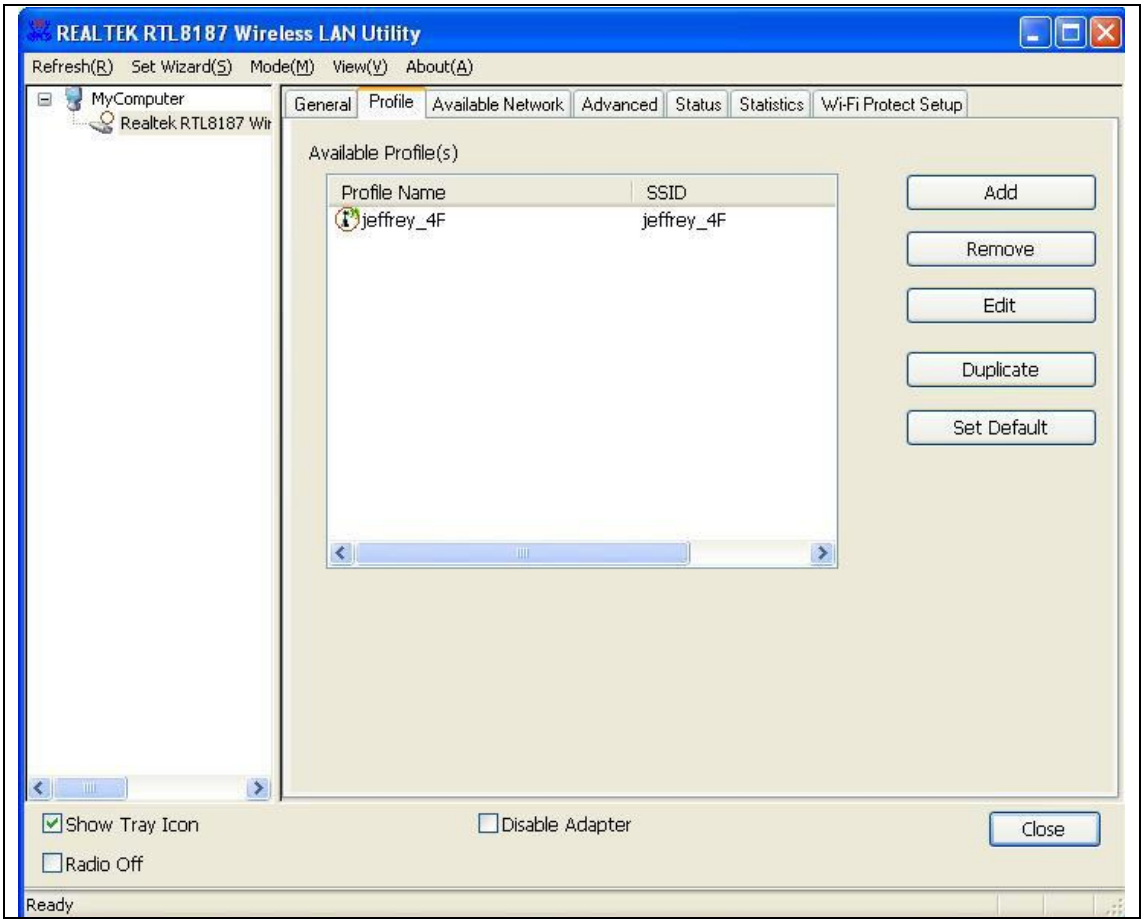
To check the connection status of the adapter, select “General“. This screen shows the information of Link Speed, Network Type, Encryption Method, SSID, Signal Strength, Link Quality and Network Address of the adapter.



Parameter	Description
Status	Shows the connection status of the adapter.
Speed	Shows the current speed
Type	**Infrastructure** – This operation mode requires the presence of an 802.11 Access Point. All communication is done via the Access Point or Router. **IBSS** – Select this mode if you want to directly connect to another wireless stations (AdHoc).
Encryption	Displays the encryption setting of the current connection. Options are None, WEP, TKIP or AES.
SSID	The SSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents unintentional merging of two co-located WLANs.
Signal Strength	Indicates the wireless signal strength.
Link Quality	Indicates the wireless link quality.
Network Address	Shows the MAC, IP address and other information of the adapter.

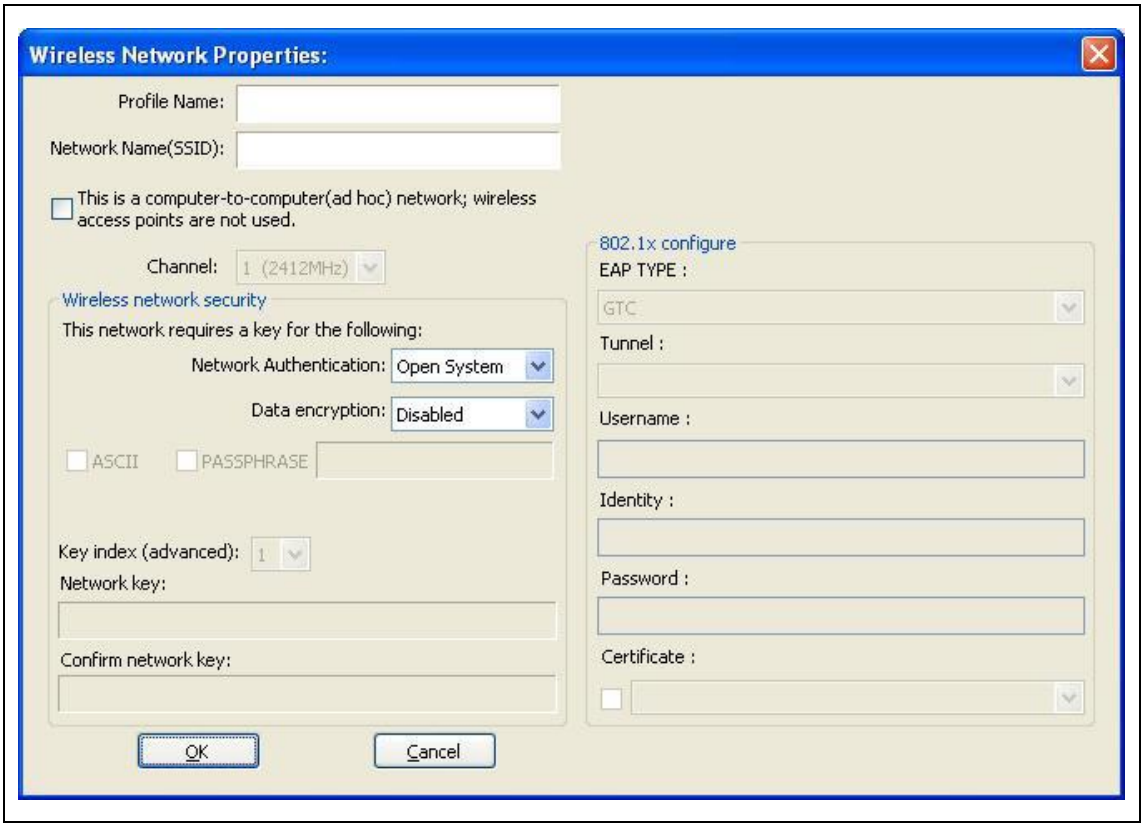
3.4 Profile

The “Profiles List” is for you to manage the networks you frequently connect to. You are able to Add/Remove/Edit/Duplicate/Set Default to manage a profile.



Parameter	Description
Available Profile(s)	A list of already added profiles and their status.
Add/Remove/Edit	Click these buttons to add/ delete/ edit profiles.
Duplicate	This is to build up a new profile with the same settings as the current profile.
Set Default	To designate a profile as the default network for wireless connection.

3.4.1 Configuring a Profile



Parameter	Description
Profile name	Define a recognizable profile name for you to identify the different networks.
Network Name (SSID)	The SSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. You may specify a SSID for the adapter and then only the device with the same SSID can interconnect with the adapter.
This is a computer-to-computer (ad-hoc) network; wireless access points are not used.	There are two types of wireless networks described below: **Infrastructure** – This operation mode requires the presence of an 802.11 Access Point. All communication is done via the Access Point or Router. **Ad Hoc** – Connect to another wireless adapter in the Wireless LAN network without going through an Access Point or Router. If this mode is selected, the adapter will work in Ad Hoc mode.
Channel	This setting is only available for Ad Hoc mode. Select the radio channel used for the network. The channel setting should be the

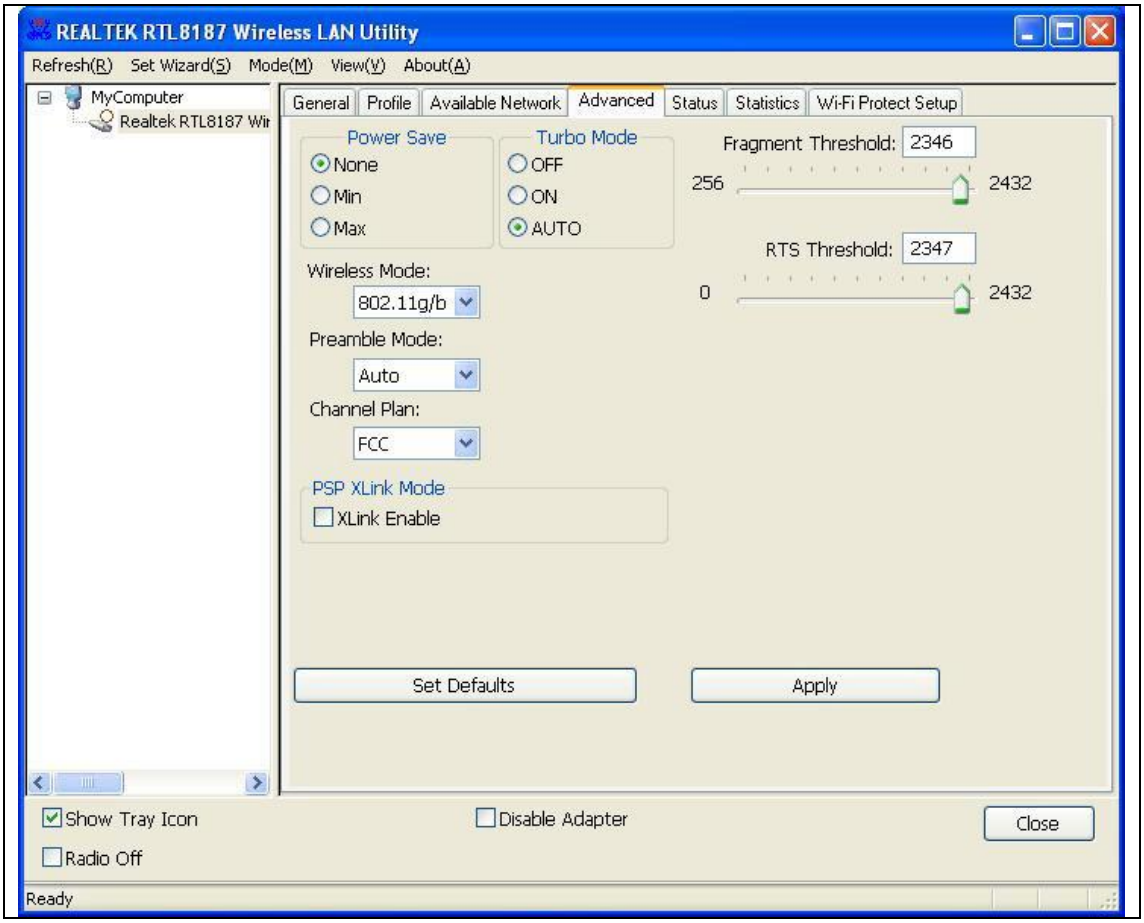
	same with the network you are connecting to.
Network Authentication	This setting has to be consistent with the wireless networks that the adapter intends to connect to. **Open System** – No authentication is needed to connect to the wireless network. **Shared Key** – Only wireless stations using a shared key (WEP Key) are allowed to connect. **WPA 802.1X** – WPA provides a scheme for mutual authentication, using either IEEE 802.1x/Extensible Authentication Protocol (EAP) authentication or pre-shared key (PSK) technology. It provides a high level of assurance to enterprise networks, small businesses and home users that data will remain protected and only authorized users may access their networks. For enterprise networks that have already deployed IEEE 802.1x authentication, WPA offers the advantage of leveraging existing authentication databases and infrastructure. **WPA-PSK** – Is a special protected access designed for home and small business users who do not have access to network authentication servers. In this mode, known as Pre-Shared Key, the user manually enters the starting password in their access point or gateway, as well as in each wireless stations in the network. WPA-PSK takes over automatically from that point, preventing unauthorized users that don't have the matching password from joining the network, while encrypting the data traveling between authorized devices. **WEP 802.1X** – It's a special mode for using IEEE 802.1x/EAP technology for authentication and WEP keys for data encryption
Data Encryption	**Disabled** – Disable Data Encryption. **WEP** – Enable WEP Encryption. When selected, you have to continue setting the WEP Encryption keys. **TKIP – TKIP** (Temporal Key Integrity Protocol) changes the temporal key every 10,000 packets (a packet is a kind of message

	transmitted over a network.) This insures much greater security than the standard WEP security. **AES – AES** has been developed to ensure the highest degree of security and authenticity for digital information and it is the most advanced solution defined by IEEE 802.11i for security in wireless networks. Note: All devices in a wireless network should use the same encryption method to ensure proper communication.
ASCII	WEP Keys can be in ASCII format. Alphanumeric values or signs are allowed to be used for WEP keys. This is more recognizable for users.
Passphrase	It is a text string with a maximum of 32 alphanumeric characters, for example: “Test“. The WEP Key is created using the Passphrase determined by you. This passphrase may not work with other vendors’ products due to possible incompatibility with that vendors’ passphrase generators. You must use the same passphrase or WEP key settings for all wireless computers within the network.
Network Key	The keys are used to encrypt data transmitted in the wireless network. Fill the text box by following the rules below. **64-bit** – Input 10 Hex digits as the encryption key. For example: “0123456aef“. **128-bit** – Input 26 Hex digits as the encryption key. For example: “01234567890123456789abcdef“.
Confirm Network Key	Enter the same network key to confirm.
Key Index (advanced)	Select one of the four keys to be the data encryption key.
EAP Type	**GTC** – GTC is an authentication protocol which allows the exchange of clear text authentication credentials across the network . **TLS** – TLS is the most secure of the EAP protocols but not easy to use. It requires that digital certificates be exchanged in the authentication phase. The server presents a certificate to the client. After validating the server’s certificate, the client presents a client certificate to the server for validation. **LEAP** – LEAP is a pre-EAP, Cisco-proprietary protocol, with many

	of the features of EAP protocols. Cisco controls the ability of other vendors to implement this protocol, so it should only be selected for use when limited vendor choice for client, access-point, and server products is not a concern. When you have set up LEAP authentication, you have to enter the user name and password of your computer. **PEAP & TTLS** – PEAP and TTLS are similar and easier than TLS, in the way that they specify a stand-alone authentication protocol be used within an encrypted tunnel. TTLS supports any protocol within its tunnel, including CHAP, MSCHAP, MSCHAPv2 and PAP. PEAP specifies that an EAP-compliant authentication protocol must be used; this adaptor supports MD5, TLS, GTC (Generic Token Card) and MSCHAPv2. The client certificate is optional for the authentication.
Tunnel	Includes MD5, GTC, TLS, CHAP, MSCHAP, MSCHAP-v2 and PAP.
Username	The certificate username in the RADIUS server.
Identity	User's identity in the RADIUS server.
Password	User's password in the RADIUS server.
Certificate	The certificate for RADIUS server for certification.

3.5 Advanced

The **"Advanced"** tab enables you to configure more advanced settings, for example: Power Save, Turbo Mode, Wireless Mode and etc.

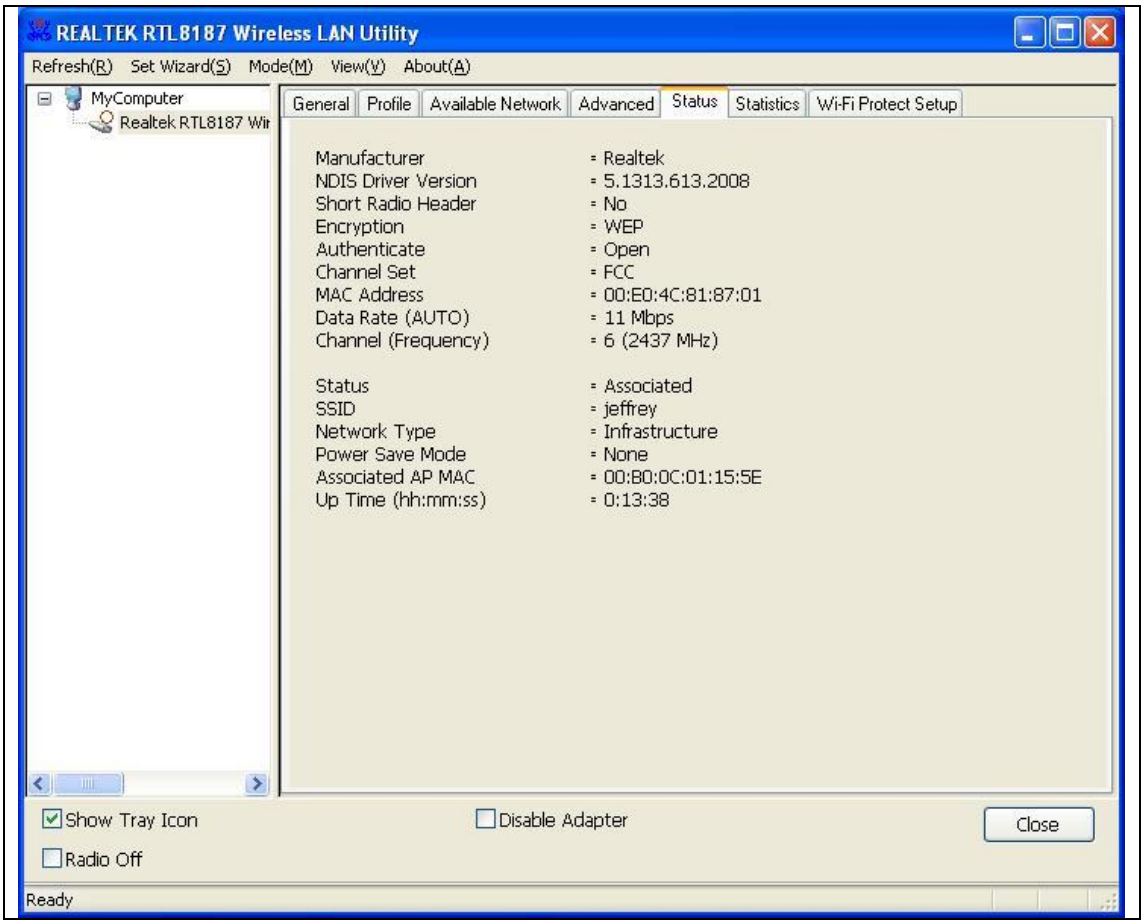


Parameter	Description
Power Save	**None** – The adapter is always set in active mode. **Min** – Switch the adapter to power saving mode when it is Idle (some components of the adapter are still active). In this mode, the power consumption is more than "Max" mode. **Max** – Switch adapter to power saving mode when idle
Turbo Mode	**Off** – Turn off the turbo mode. **On** – Turn on the turbo mode. **Auto** – The adapter will detect to see if AP is RTL8186-based or Not. If yes, it will transmit data in turbo mode automatically.
Wireless Mode	**802.11 b** – This adapter is compatible with both 802.11g and

	802.11b wireless stations. If there are only 802.11b wireless stations in the network, you can set the adapter to this mode. **802.11 g/b** – If you have a mix of 802.11b and 802.11g wireless stations in your network.
Preamble	The preamble defines the length of the CRC block for communication among wireless stations. There are three modes including Long, Short and Auto. High network traffic areas should use the shorter preamble type. If “Auto“ mode is selected, the adapter will auto switch the preamble mode depending on the wireless stations that the adapter is connecting to. Note that the parameter is only active in the Ad Hoc operation mode.
Channel Plan	Please select local channel from the drop down list
PSP XLink Mode	Enable this function to support PSP XLink.
Fragment Threshold	The value defines the maximum size of packets; any packet size larger than the value will be fragmented. If you have decreased this value and experience high packet error rates, you can increase it again, but it will likely decrease overall network performance. Select a setting within a range of 256 to 2432 bytes. Minor change is recommended.
RTS Threshold	Minimum packet size required for an RTS (Request To Send). For packets smaller than this threshold, an RTS is not sent and the packet is transmitted directly to the wireless network. Select a setting within a range of 0 to 2432 bytes. Minor change is recommended.
Set Default	Let the setting values return to default.
Apply	Confirm the settings in the “Advanced“.

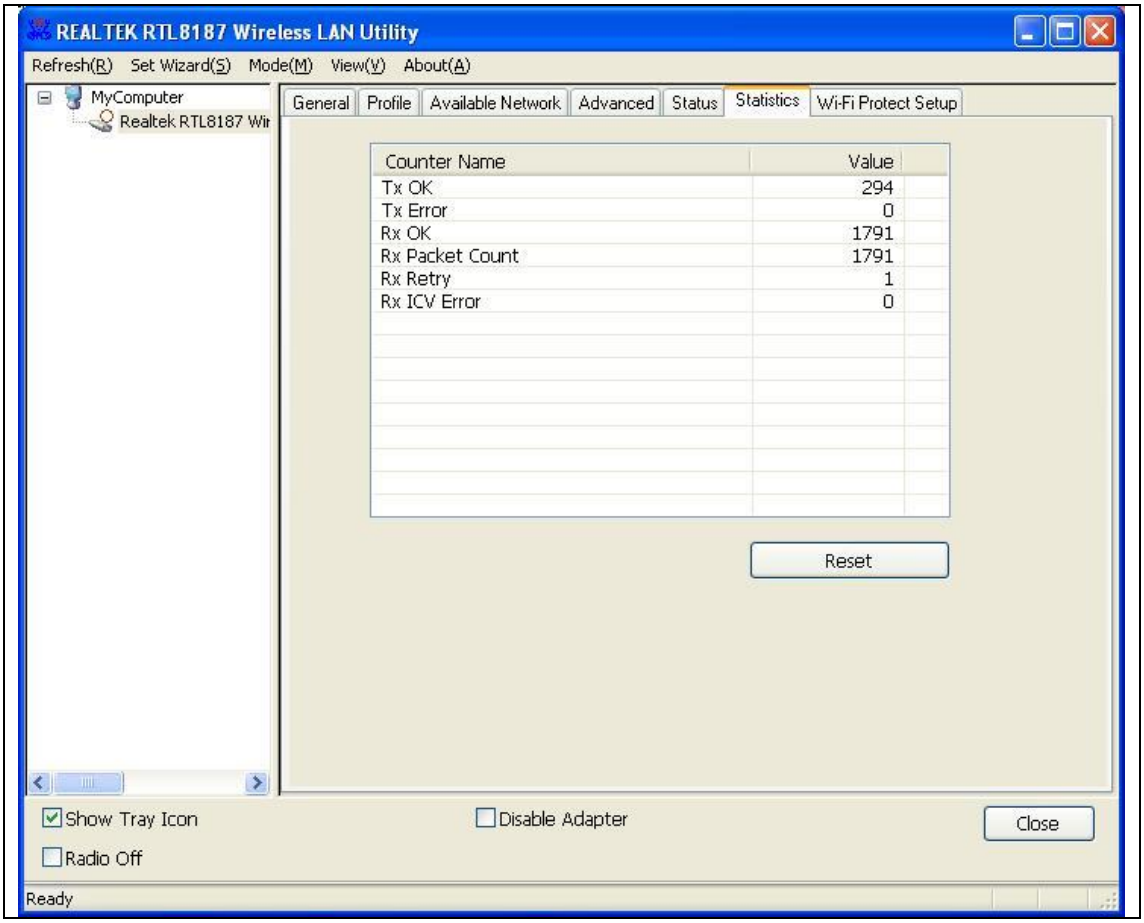
3.6 Status

This screen shows the information of the chipset manufacturer, driver version, settings of the wireless network the adapter is connecting to, linking time and link status. If you're not sure about the status of the adapter and the network you are connecting, please go to the screen for more details.



3.7 Statistics

You can get real time information about the packet transmission and receiving status during wireless communication from the screen. If you want to recount, please click **"Reset"**.

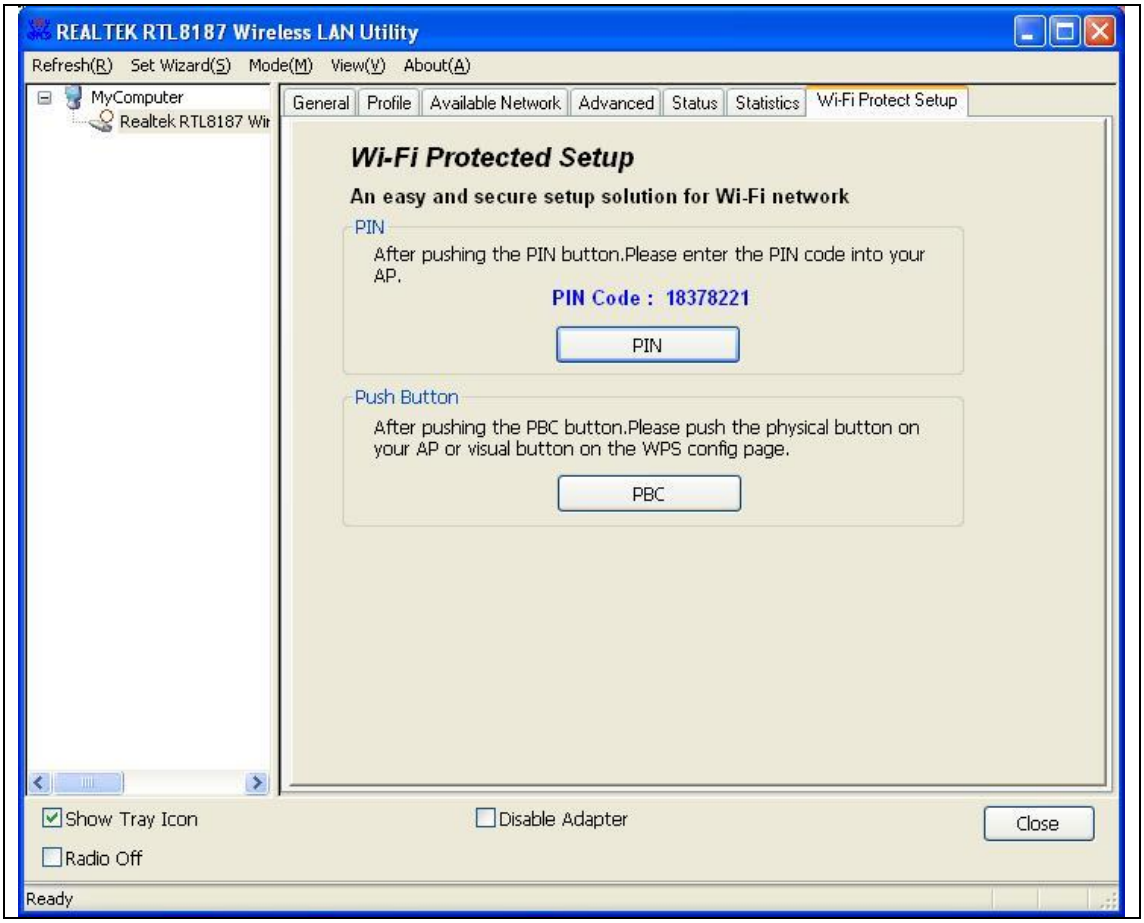


3.8 Wi-Fi Protect Setup

Wi-Fi Protected Setup (WPS) is the latest wireless network technology, which makes wireless network setup, become very simple. If you have WPS-enabled wireless access point, and you want to establish a secure connection to it, you don't have to configure the wireless access point and setup data encryption by yourself. All you have to do is to go to the WPS setup page of this wireless card, click a button, and then press a specific button or enter a set of 8-digit code on the wireless access point you wish to establish a secure connection - just three simple steps!

For older wireless access points, it's possible to perform a firmware upgrade to become a WPS-enabled access point. Since they may not have a hardware button to press for WPS setup, you can use an alternative WPS setup method - input the pin code. Every WPS-compatible wireless network card supports pin code configuration method; you can just input the code to wireless access point, and the wireless access point and wireless network card will do the rest for you.

This wireless network card is compatible with WPS. To use this function, the wireless access point you wish to connect to must support WPS function too. Now, please follow the following instructions to establish secure connection between WPS-enabled wireless access point and your wireless network card.


REALTEK RTL8187 Wireless LAN Utility
Refresh(R) Set Wizard(S) Mode(M) View(V) About(A)
MyComputer
Realtek RTL8187 Wir
General Profile Available Network Advanced Status Statistics Wi-Fi Protect Setup
Wi-Fi Protected Setup
An easy and secure setup solution for Wi-Fi network
PIN
After pushing the PIN button.Please enter the PIN code into your AP.
PIN Code : 18378221
PIN
Push Button
After pushing the PBC button.Please push the physical button on your AP or visual button on the WPS config page.
PBC
Show Tray Icon
Disable Adapter
Close
Radio Off
Ready

3.8.1 WPS Setup – PIN

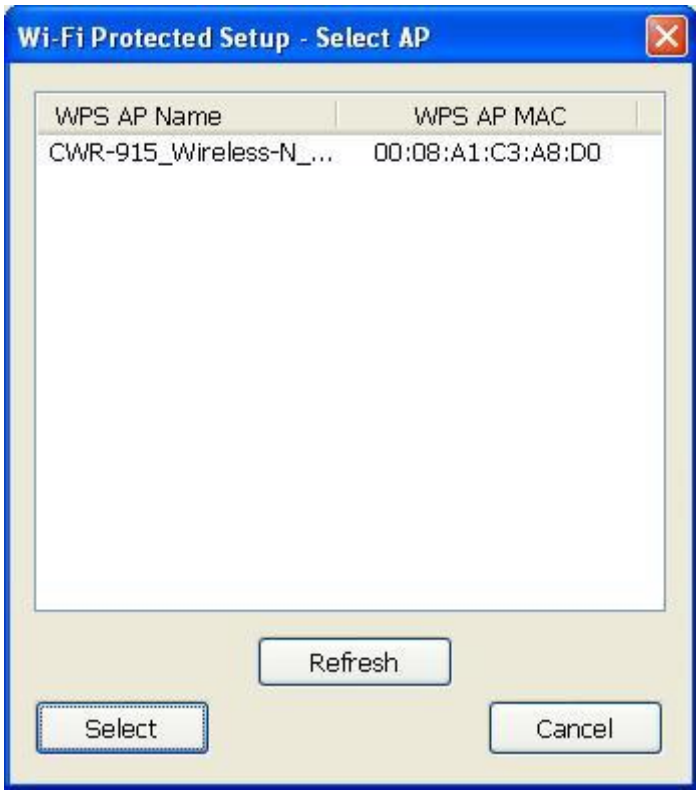
If the wireless access point you wish to connect supports PIN, please follow the following instructions to establish connection to it:

1. Click **"Wi-Fi Protect Setup"** page
2. The PIN code of your wireless network card is an eight-digit number located at the upper position of configuration utility. Remember it, and input the number to your wireless access point as the WPS PIN code (Please refer to the user manual of your wireless access point for instructions about how to do this)

Wi-Fi Protected Setup
An easy and secure setup solution for Wi-Fi network
PIN
After pushing the PIN button.Please enter the PIN code into your AP.
PIN Code : 79696463
PIN
Push Button
After pushing the PBC button.Please push the physical button on your AP or visual button on the WPS config page.
PBC

3. Click **'PIN'** button, device will show the following message. Please click **"Yes"** to search router/access point.

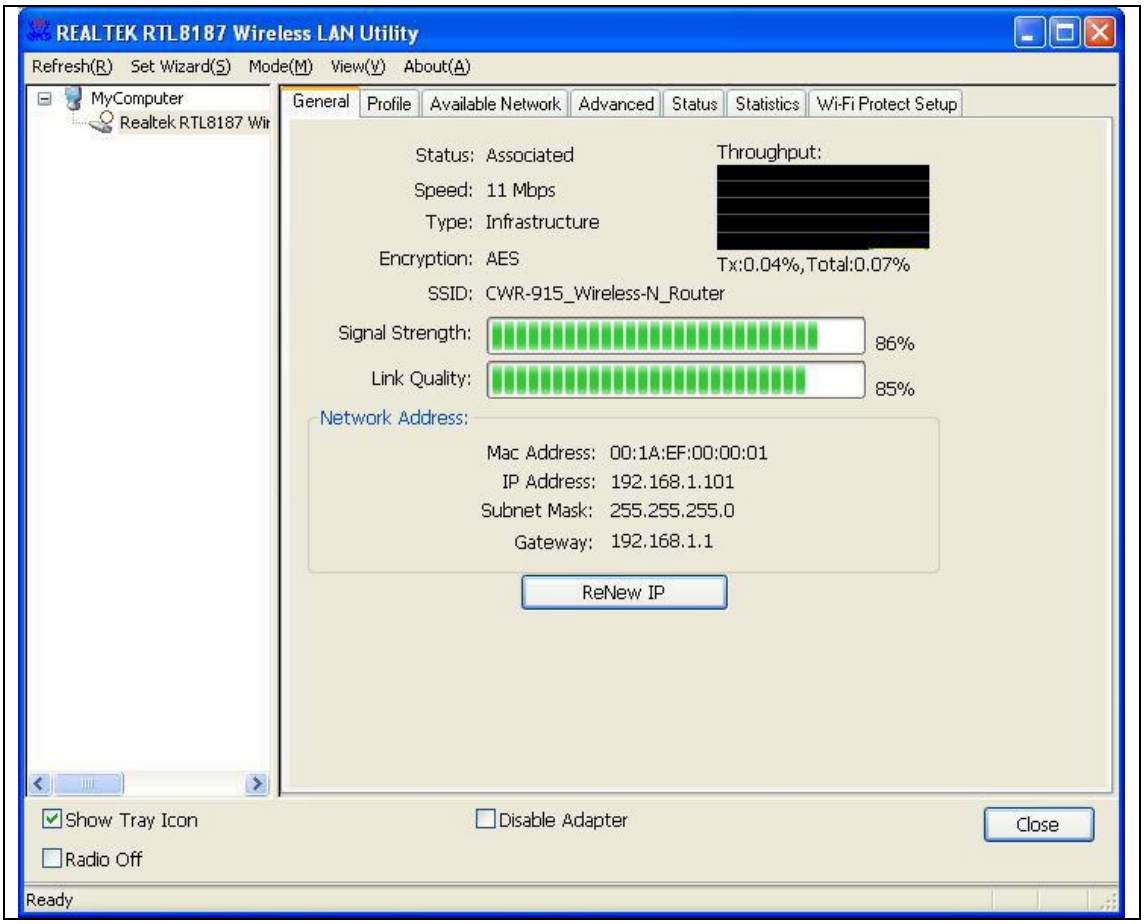
4. It will show the router/access point name with enabled WPS function in the list. Select the AP Name and click **"Select"** to continue the process.



5. It will start WPS process, please wait from a few second to two minutes. If wireless router/access point with correct code is found, you'll be connected to that router/access point.

Wi-Fi Protected Setup - PIN method
Wi-Fi Protected Setup - PIN method
Please enter the following PIN code into your AP .
PIN Code : 79696463
Status : [CWR-915_Wireless-N_Router] WPS Protocol
Cancel

6. After configuring successfully, you will see connection information in the **"General"** page.



3.8.2 WPS Setup – PBC (Push Button Configuration)

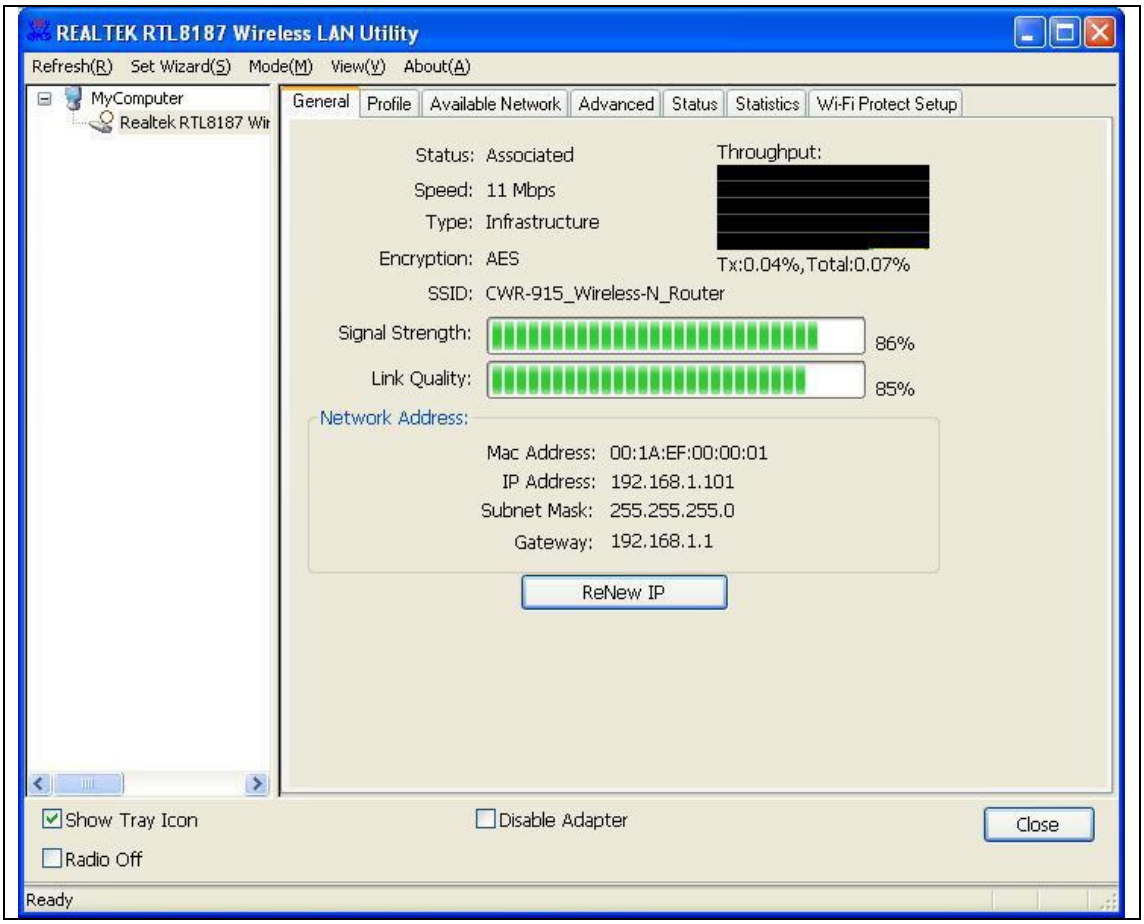
1. Click **"Wi-Fi Protect Setup"** page
2. Click "PBC" button to start WPS process.

Wi-Fi Protected Setup
An easy and secure setup solution for Wi-Fi network
PIN
After pushing the PIN button.Please enter the PIN code into your AP.
PIN Code : 79696463
PIN
Push Button
After pushing the PBC button.Please push the physical button on your AP or visual button on the WPS config page.
PBC

3. Start PBC pairing procedure at access point side (please refer to the instruction given by your access point's manufacturer), then click '**PBC**' button in wireless configuration utility to start to establish wireless connection by WPS. Please be patient (This may require several seconds to one minute to complete).

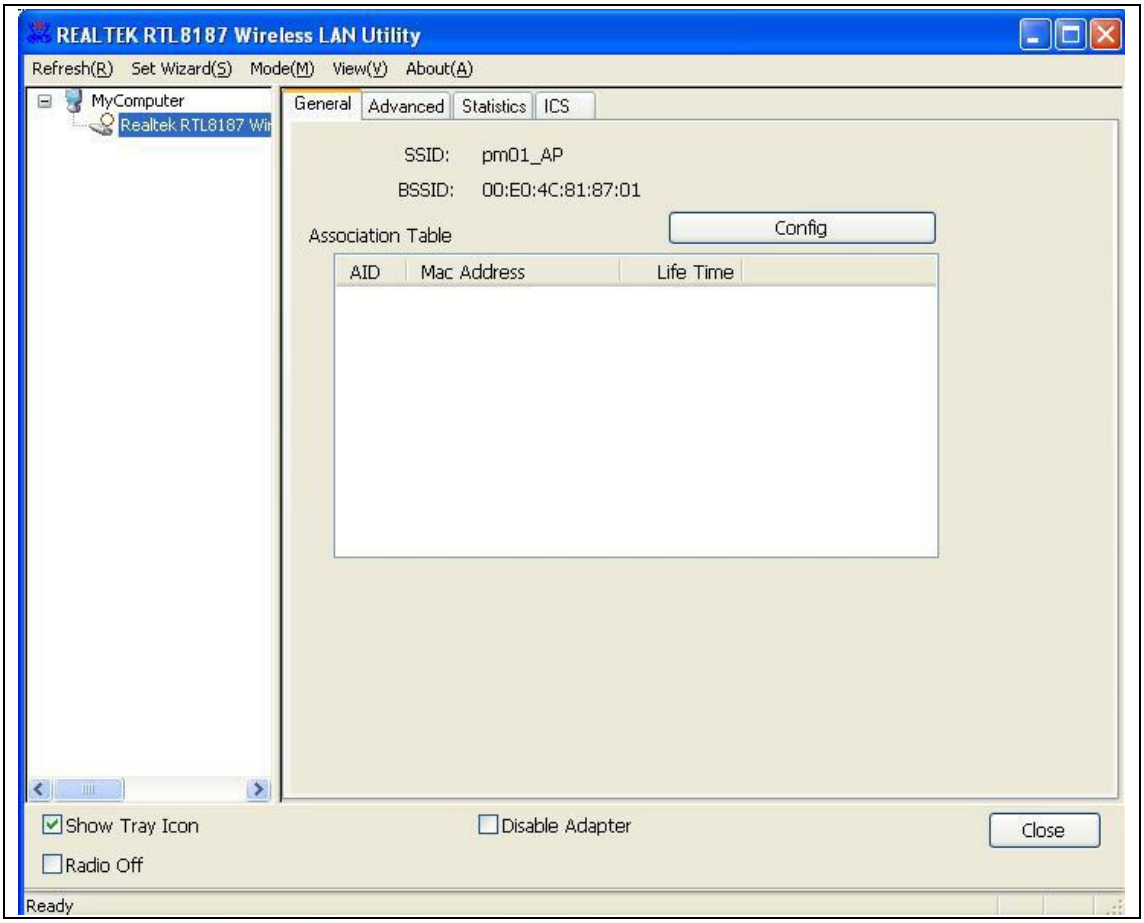
Wi-Fi Protected Setup - PBC method
Wi-Fi Protected Setup - PBC method
If there is more then one AP on the PBC mode,there will be "Session Overlap".Please using PIN method or wait for a while push the button again.
Status : WPS Protocol Communication ...
Complete :
PBC
Cancel

4. After configuring successfully, you will see connection information in the **"General"** page.



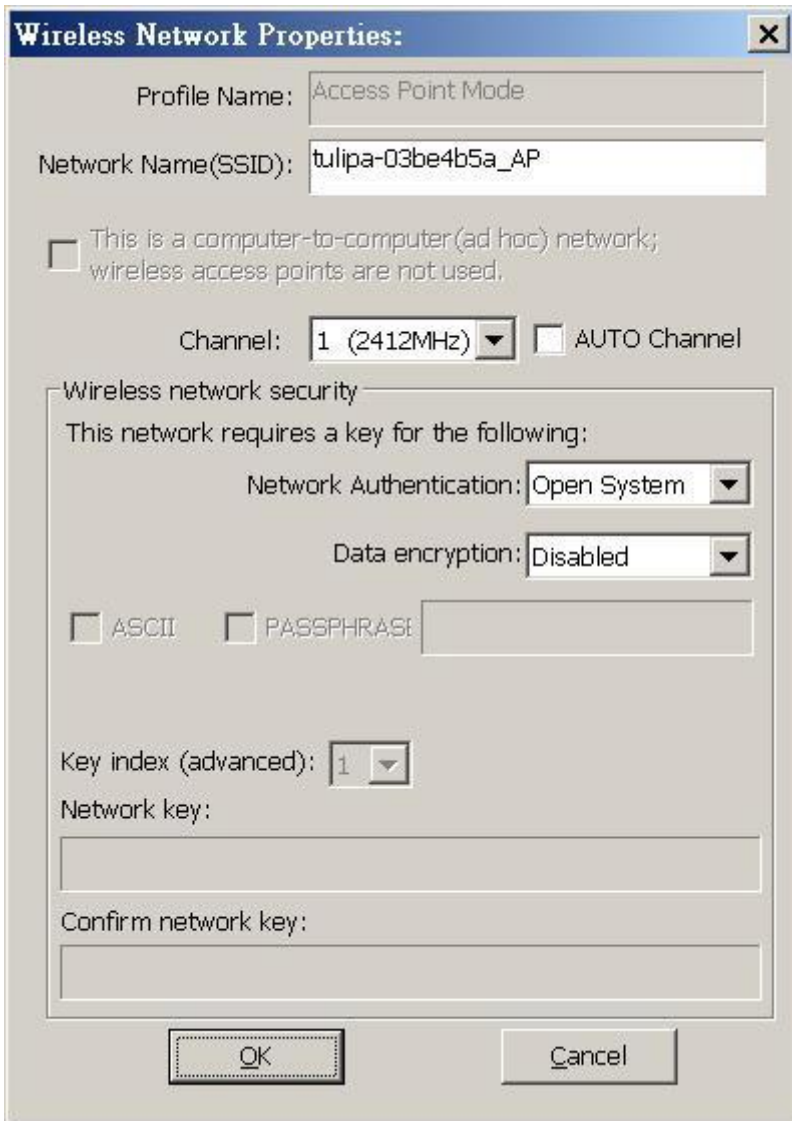
3.9 Software AP

This adapter can run as a wireless AP. The relative configurations of the AP including channel, SSID, WEP encryption and so on are described below.



Parameter	Description
SSID	The SSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. The default SSID of the AP is Full Computer Name + "_AP". Wireless adapters connecting to the AP should set up the same SSID as the AP.
BSSID	Displays the MAC address of the adapter.
Association Table	All the wireless adapters connected to the software AP will be displayed in the list.
Config	Click **"Config"** for configuring more settings on the AP.

3.9.1 AP Properties Setting

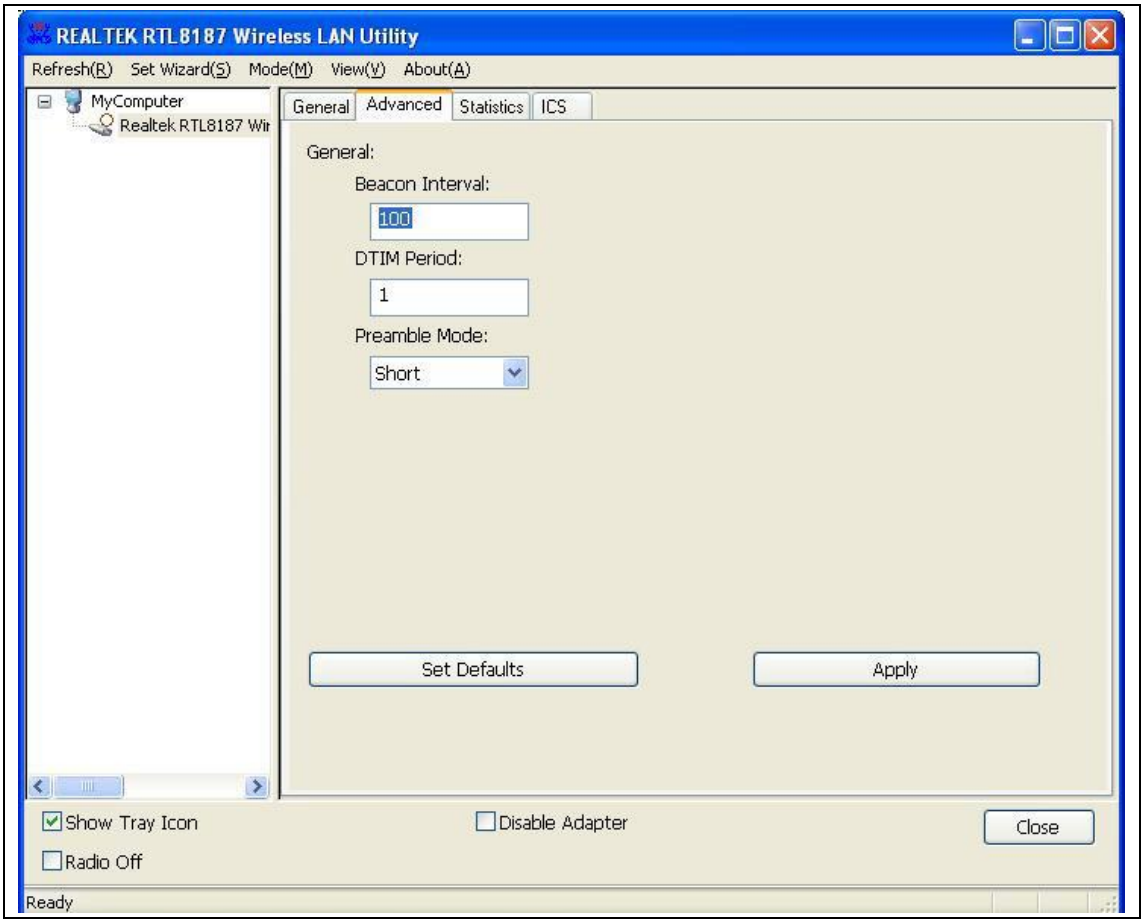


Parameter	Description
Profile name	Define a recognizable profile name for you to identify different networks.
Network Name (SSID)	The SSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. You may specify a SSID for the adapter and then only the device with the same SSID can interconnect with the adapter.
Channel	This setting is only available for Ad Hoc mode. Select the channel number used for the network. The channel setting should be the

	same with the network you are connecting to.
Network Authentication	This setting has to be consistent with the wireless networks that the adapter intends to connect to. **Open System** – No authentication is needed to connect to the wireless network. **Shared Key** – Only wireless stations using a shared key (WEP Key) are allowed to connect to each other. **WPA-PSK** – Is a special protected access designed for home and small business users who do not have access to network authentication servers. In this mode, known as Pre-Shared Key, the user manually enters the starting password in their access point or gateway, as well as in each wireless stations in the network. WPA-PSK takes over automatically from that point, preventing unauthorized users that don't have the matching password from joining the network, while encrypting the data traveling between authorized devices. **WPA2-PSK** – WPA2-PSK is also for home and small businesses. The difference between WPA-PSK and WPA2-PSK is that WPA2-PSK provides data encryption via AES. In contrast, WPA-PSK uses Temporal Key Integrity Protocol (TKIP).
Data Encryption	**Disabled** – Disable the WEP Encryption. **WEP** – Enable WEP Encryption. When WEP is selected, you have to continue setting the WEP keys. **TKIP – TKIP** (Temporal Key Integrity Protocol) changes the temporal key every 10,000 packets (a packet is a kind of message transmitted over a network.) This insures much greater security than the standard WEP security. **AES – AES** has been developed to ensure the highest degree of security and authenticity for digital information and it is the most advanced solution defined by IEEE 802.11i for security in wireless networks. Note: All devices in the network should use the same encryption method to ensure proper communication.

ASCII	WEP Keys can be in ASCII format. Alphanumeric values or signs are allowed to be used. This format is more recognizable for users.
Passphrase	It is a text string with a maximum of 32 alphanumeric characters, for example: “Test“. The WEP Key is created based on the Passphrase entered. This passphrase may not work with other vendors’ products due to possible incompatibility with their passphrase generators. You must use the same passphrase or WEP key settings for all wireless computers within the network.
Network Key	The keys are used to encrypt data transmitted in the wireless network. Fill the text box by following the rules below. **64-bit** – Input 10 Hex digits as the encryption key. For example: “0123456aef“. **128-bit** – Input 26 Hex digits as the encryption key. For example: “01234567890123456789abcdef“.
Confirm Network Key	Enter the same network key to confirm.
Key Index (advanced)	Select one of the four keys to be the data encryption key.

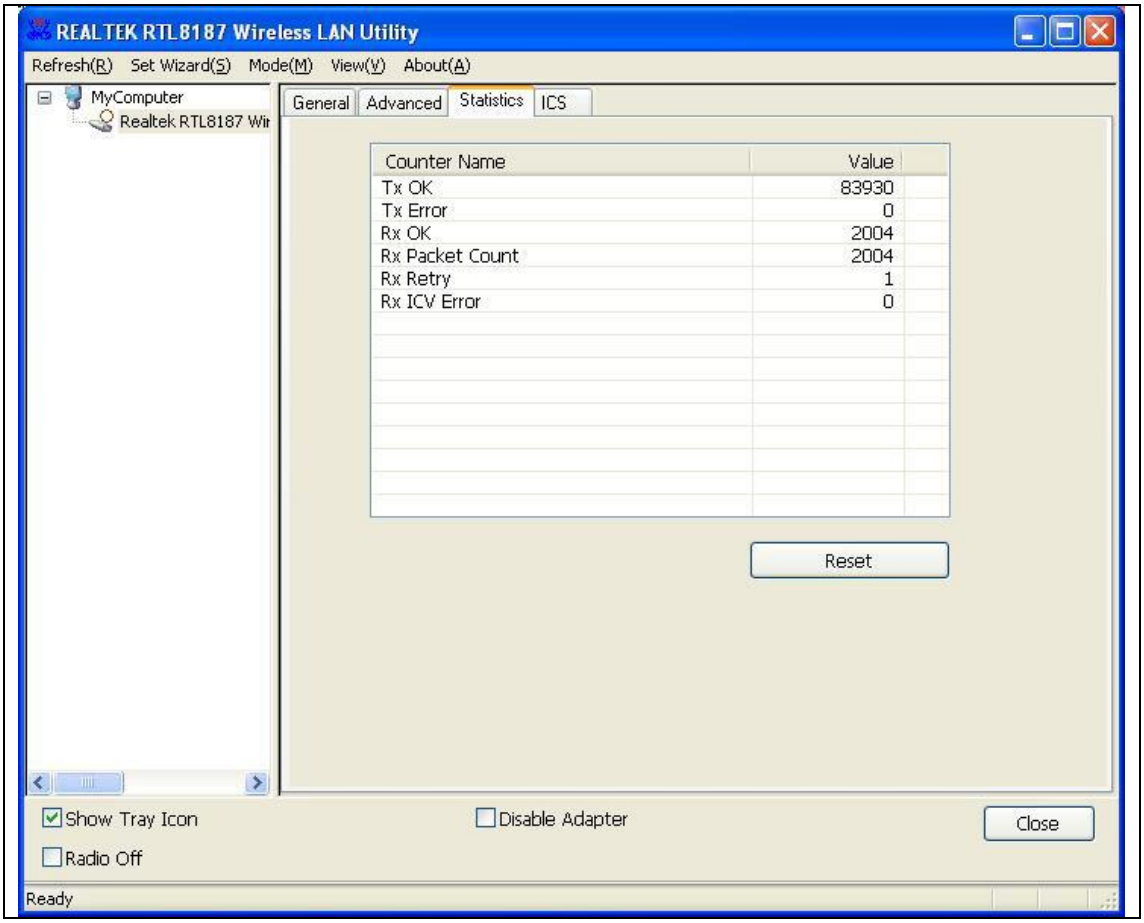
3.9.2 AP Advanced



Parameter	Description
Beacon Interval	Beacon Interval specifies the duration between beacon packets (milliseconds). The range for the beacon period is between 20-1000 milliseconds with a typical value of 100.
DTIM Period	Determines the interval the Access Point will send its broadcast traffic. Default value is 3 beacons.
Preamble Mode	The preamble defines the length of the CRC block for communication among wireless stations. There are three mode including Long, Short and Auto. High network traffic areas should use the shorter preamble type. If “Auto“ mode is selected, the AP will auto switch the preamble mode depending on the wireless adapters.
Set Default	Set values to defaults.
Apply	Confirm settings in the **“Advanced“**.

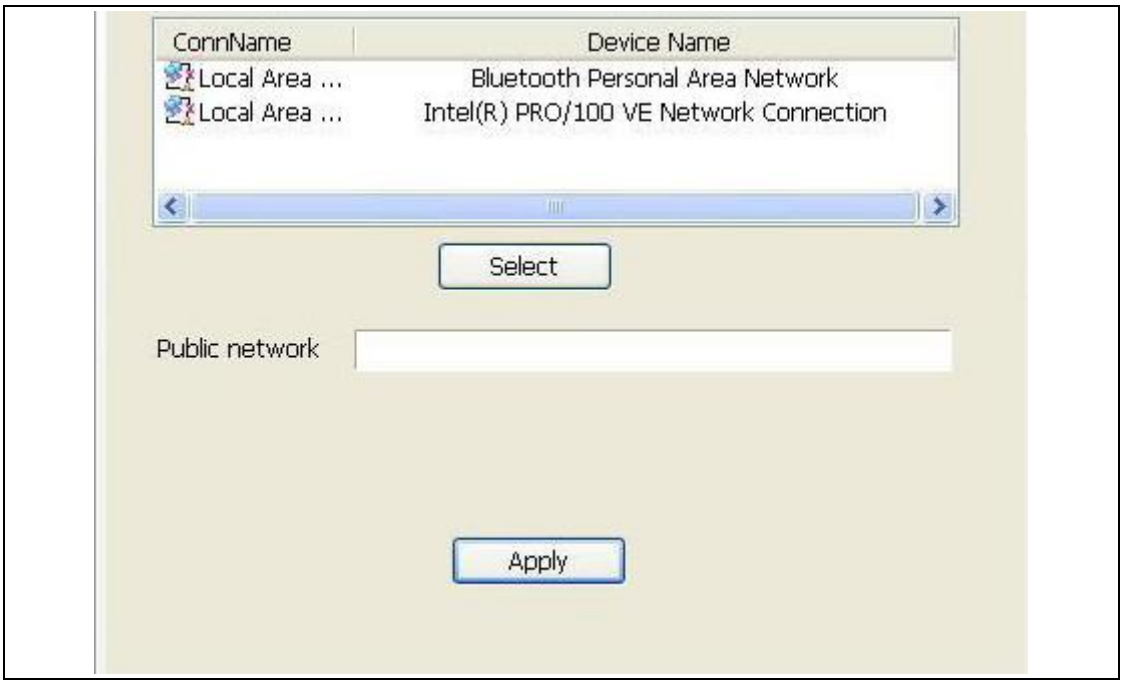
3.9.3 AP Statistics

You can get real time information about the packet transmission and receiving status from this screen. If you want to restart the counters, please click **"Reset"**.



3.9.4 ICS

If you want to connect to the Internet through this SoftAP, you will need to make a bridge between the SoftAP and your Internet connection device. Select the Internet connection in your SoftAP host machine and press the **"Apply"** button.

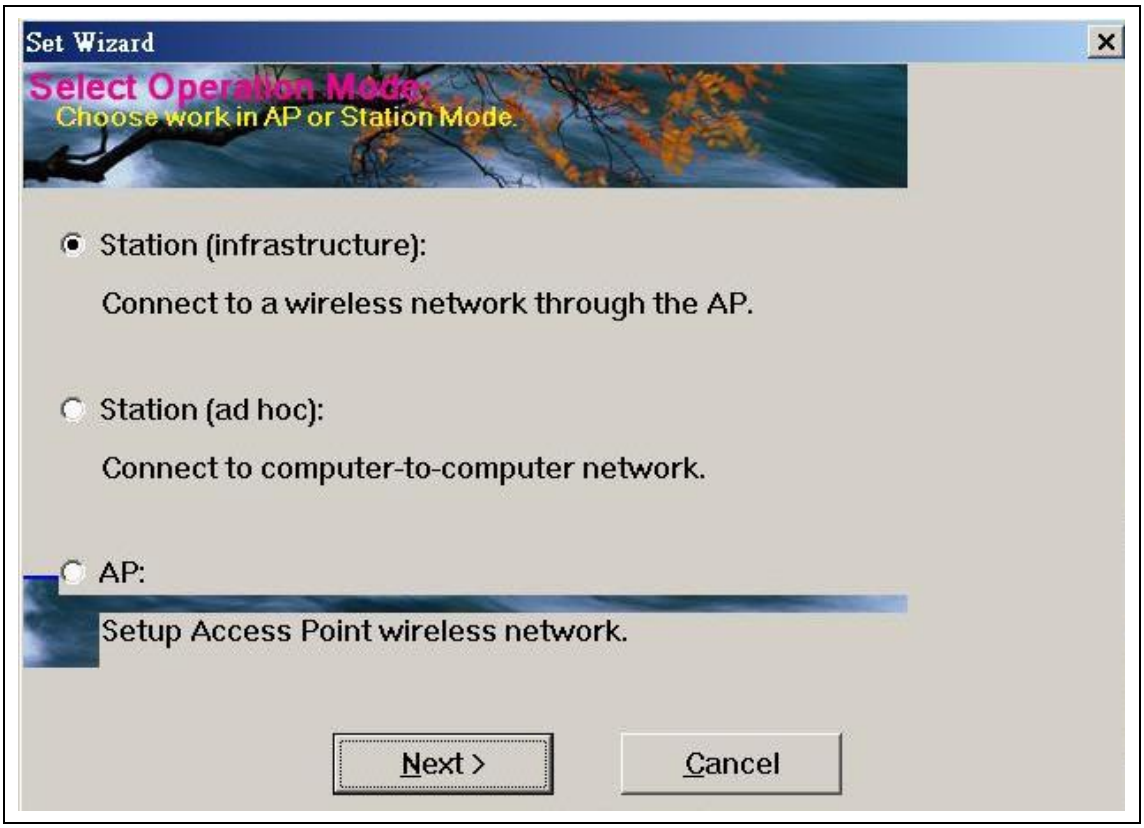


Chapter 4 Set Wizard

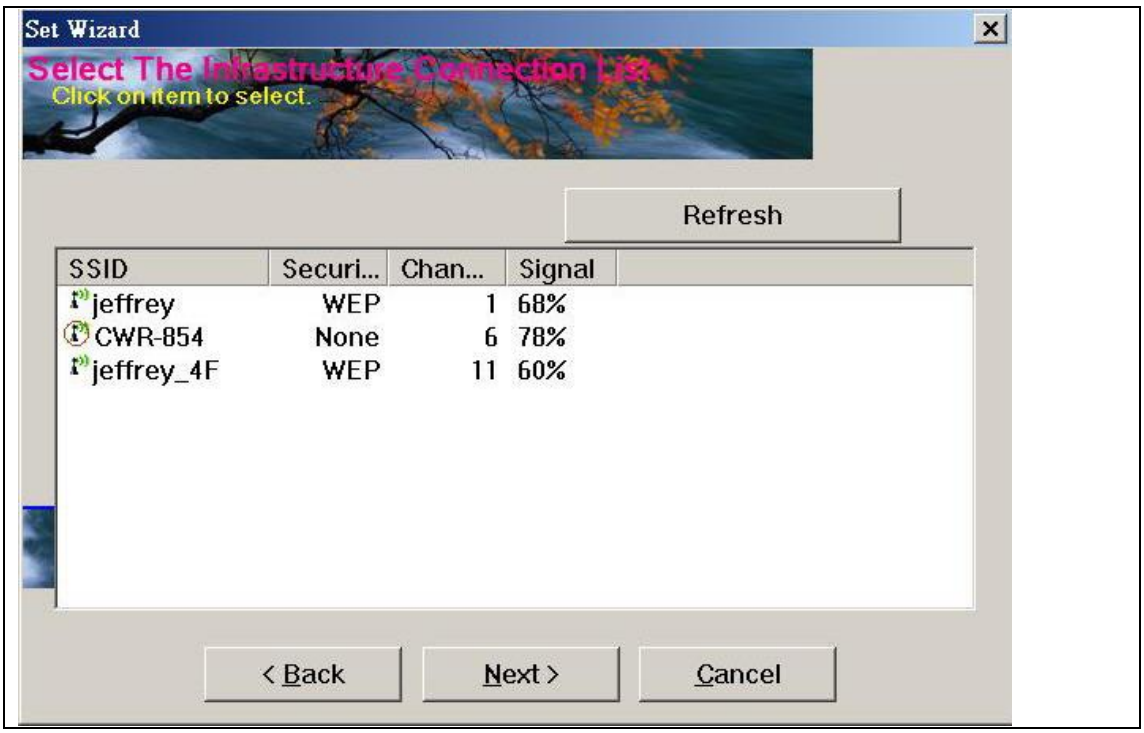
The Set Wizard can help users to connect to a wireless LAN or build an Ad-hoc wireless network.

For example, if you want to connect to a wireless LAN in infrastructure mode:

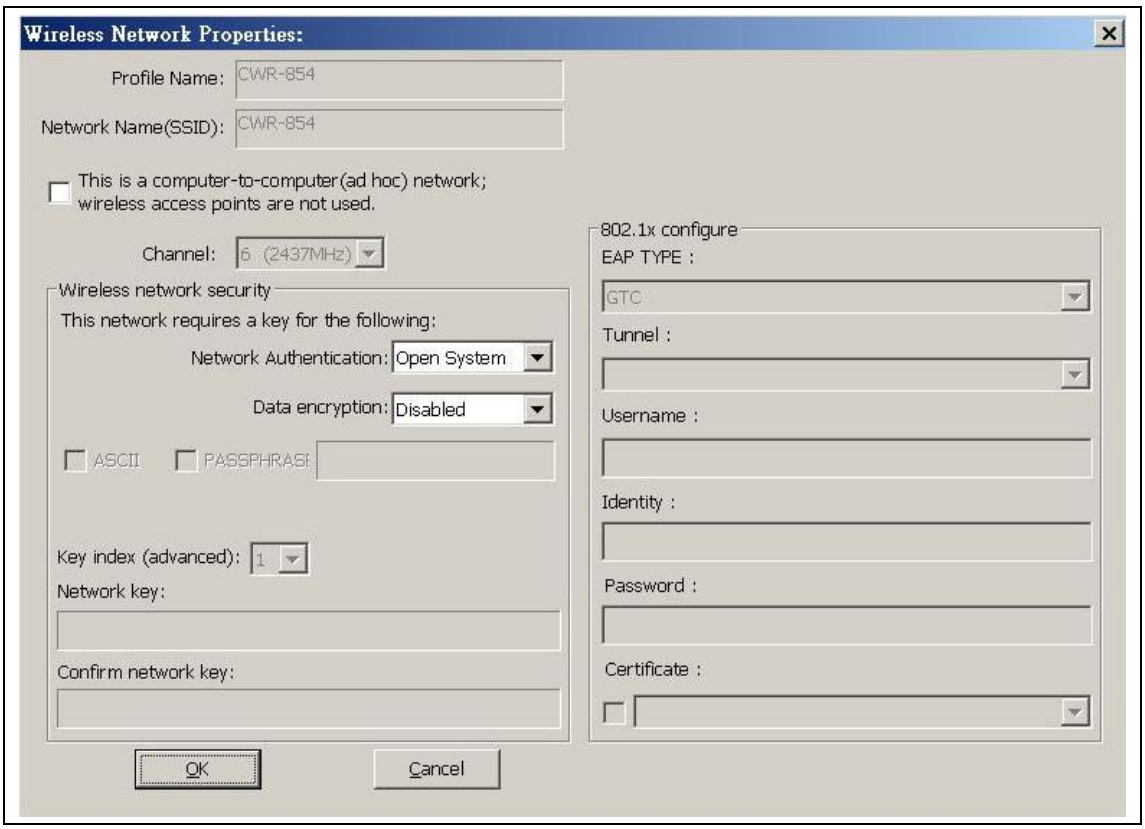
A. Open the Set Wizard and choose the Station (infrastructure) mode.



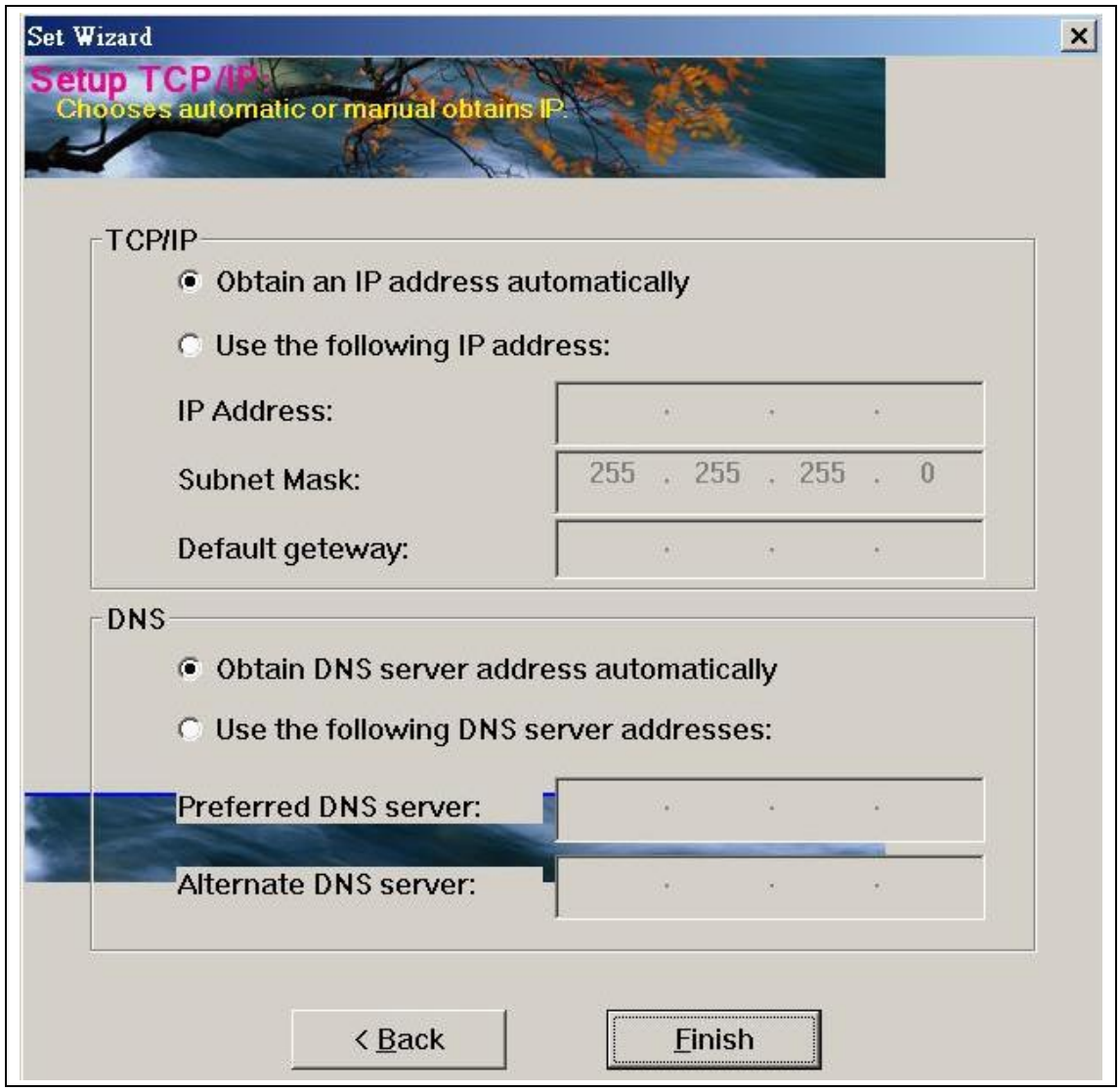
B. The site survey results will show up. Please select the SSID you'd like to connect to and click the **"Next"** button.



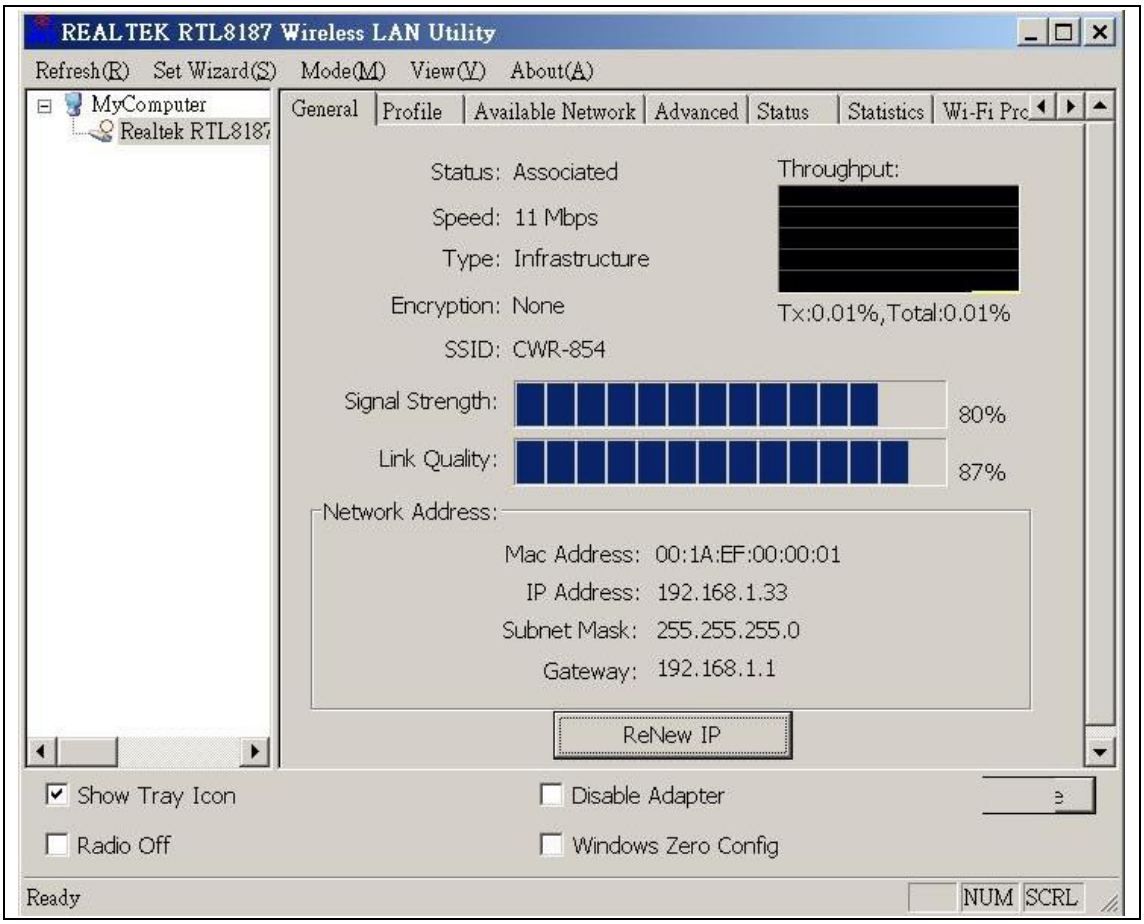
C. In the Wireless network properties dialog, please fill in the security settings for this wireless network you'd like to connect to.



D. Please fill related IP information for this wireless network and click the **"Finish"** button.



E. Now you can connect to the wireless network successfully.



Chapter 5 Glossary

1. What is the IEEE 802.11g standard?

802.11g is an IEEE standard for high-speed wireless LAN communications that provides up to 54 Mbps data rate in the 2.4 GHz band. 802.11g is the mainstream wireless LAN technology for home, office and public networks.

802.11g define the use of the same OFDM modulation technique specified in IEEE 802.11a for the 5 GHz frequency band and applies it in the same 2.4 GHz frequency band as IEEE 802.11b. The 802.11g standard require backward compatibility with 802.11b.

The standard specifically calls for:

A. A new physical layer for the 802.11 Medium Access Control (MAC) in the 2.4 GHz frequency band, known as the extended rate PHY (ERP). The ERP adds OFDM as a mandatory new coding scheme for 6, 12 and 24 Mbps (mandatory speeds), and 18, 36, 48 and 54 Mbps (optional speeds). The ERP includes the modulation schemes found in 802.11b including CCK for 11 and 5.5 Mbps and Barker code modulation for 2 and 1 Mbps.

B. A protection mechanism called RTS/CTS that governs how 802.11g devices and 802.11b devices interoperate.

2. What is the IEEE 802.11b standard?

The IEEE 802.11b Wireless LAN standard subcommittee, which formulates the standard for the industry. The objective is to enable wireless LAN hardware from different manufactures to communicate.

3. What does IEEE 802.11 feature support?

The product supports the following IEEE 802.11 functions:

- CSMA/CA plus Acknowledge Protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS Feature
- Fragmentation
- Power Management

4. What is Ad-hoc?

An Ad-hoc integrated wireless LAN is a group of computers, each has a Wireless LAN card, Connected as an independent wireless LAN. Ad hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

5. What is Infrastructure?

An integrated wireless and wireless and wired LAN is called an Infrastructure configuration. Infrastructure is applicable to enterprise scale for wireless access to central database, or wireless application for mobile workers.

6. What is BSS ID?

A specific Ad hoc LAN is called a Basic Service Set (BSS). Computers in a BSS must be configured with the same BSS ID.

7. What is WEP?

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 40 bit shared key algorithm, as described in the IEEE 802 .11 standard.

8. What is TKIP?

TKIP is a quick-fix method to quickly overcome the inherent weaknesses in WEP security, especially the reuse of encryption keys. TKIP is involved in the IEEE 802.11i WLAN security standard, and the specification might be officially released by early 2003.

9. What is AES?

AES (Advanced Encryption Standard), a chip-based security, has been developed to ensure the highest degree of security and authenticity for digital information, wherever and however communicated or stored, while making more efficient use of hardware and/or software than previous encryption standards. It is also included in IEEE 802.11i standard. Compare with AES, TKIP is a temporary protocol for replacing WEP security until manufacturers implement AES at the hardware level.

10. Can Wireless products support printer sharing?

Wireless products perform the same function as LAN products. Therefore, Wireless products can work with Netware, Windows 2000, or other LAN operating systems to support printer or file sharing.

11. Would the information be intercepted while transmitting on air?

WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, WLAN series offer the encryption function (WEP) to enhance security and Access Control. Users can set it up depending upon their needs.

12. What is DSSS? What is FHSS? And what are their differences?

Frequency-hopping spread-spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-sequence spread-spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip is, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without-the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

13. What is Spread Spectrum?

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communication systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread –spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

14. What is WPS?

WPS stands for Wi-Fi Protected Setup. It provides a simple way to automatically establish unencrypted or encrypted connections between wireless clients and access point. User can press a software or hardware button to activate WPS function, and WPS-compatible wireless clients and access point will establish connection by themselves. There are two types of WPS: PBC (Push-Button Configuration) and PIN code.